2/2014

# Datenschutz Nachrichten

37. Jahrgang
ISSN 0137-7767
12,00 Euro

Das Internet der Dinge

■ TTIP – Freier Handel, unfreie Bürger? ■ Das Internet der Dinge ■ Smart Meters ■ IPv6 und Privatsphäre ■ Weshalb Deutschland Edward Snowden um Einreise bitten muss ■ Diese Geheimdienste sind nicht reformierbar ■ Kirchensteuersperrvermerk ■ BigBrotherAwards 2014 ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

# Inhalt



# Termine

23. Juni 2014, 09:00 Uhr - 24. Juni 2014, 17:00 Uhr
**DuD 2014 - Fachkonferenz**
**Datenschutz & Datensicherheit**
16. COMPUTAS-Jahresfachkonferenz
Leonardo Royal Hotel Berlin

Sonntag, 06. Juli 2014, 10:00 Uhr
**DVD-Vorstandssitzung**
Berlin. Anmeldung in Geschäftsstelle
dvd@datenschutzverein.de

Freitag, 01. August 2014
**Redaktionsschluss DANA 3/2014**
Thema: Datenschutz an Flughäfen
Verantwortlich: Frans Valenta

Donnerstag, 18. September 2014, 09:30 Uhr
**BvD-Datenschutz-Symposium - 25 Jahre BvD**
Maritim Hotel Ulm

Samstag, 18. Oktober 2014, 16:00 Uhr
**DVD-Vorstandssitzung**
Bonn. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Sonntag, 19. Oktober 2014, 10:00 Uhr
**Mitgliederversammlung**
Bonn. Gesonderte Einladung folgt. Anmeldung in der Geschäftsstelle erbeten

Samstag, 01. November 2014
**Redaktionsschluss DANA 4/2014**
Thema: Big Data
Verantwortlich: Jaqueline Rüdiger

**DANA**
**Datenschutz Nachrichten**
ISSN 0137-7767
37. Jahrgang, Heft 2

**Herausgeber**
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Rheingasse 8-10, 53113 Bonn
Tel. 0228-222498
Konto 1900 2187, BLZ 370 501 98, Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

**Redaktion (ViSdP)**
Frank Spaeing
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Rheingasse 8-10, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

**Layout und Satz**
Frans Jozef Valenta, 53119 Bonn
valenta@t-online.de

**Druck**
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0)91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

**Bezugspreis**
Einzelheft 12 Euro. Jahresabonnement 42 Euro (incl. Porto) für vier Hefte im Jahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

**Copyright**
Die Urheber- und Vervielfältigungsrechte liegen bei den Autoren. Der Nachdruck ist nach Genehmigung durch die Redaktion bei Zusendung von zwei Belegexemplaren nicht nur gestattet, sondern durchaus erwünscht, wenn auf die DANA als Quelle hingewiesen wird.

**Leserbriefe**
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

**Abbildungen, Fotos**
Frans Jozef Valenta, soweit nicht anders gekennzeichnet

# Editorial

Liebe Leserinnen und Leser,

ein Jahr ist vergangen seit dem Beginn der spektakulären Enthüllungen durch Edward Snowden und seine Mitstreiter. Immer noch sitzt Edward Snowden in Russland im (zeitlich) begrenzten Asyl. Bei der Verleihung der BigBrotherAwards2014 wurde für ihn Asyl in Deutschland gefordert und auch wir veröffentlichen in dieser Ausgabe der DANA einen Artikel, der ausführlich beschreibt, warum Edward Snowden nach Deutschland eingeladen werden muss. Beachten Sie in diesem Zusammenhang bitte auch unsere aktuelle Presseerklärung zur Unreformierbarkeit der deutsche Geheimdienste.
Das transatlantische Freihandelsabkommen TTIP birgt so viel Sprengstoff für alle Europäer, man könnte wahrscheinlich schon damit ganze DANA-Ausgaben füllen. Wenn man nur wüsste, was da wirklich verhandelt werden soll. Unser Artikel versucht ein wenig Licht ins Dunkel zu bringen.

Unser Schwerpunktthema für die Ihnen vorliegende Ausgabe ist aber ein anderes: Das Internet der Dinge. Wir haben versucht, mehrere Facetten zu beleuchten, angefangen bei einem Artikel über Smart Meter, die in der momentan durch die Regierung und Wirtschaft favorisierten Konzeption umfangreiche Auskünfte über unser Leben ermöglichen. Weiter haben wir einen Artikel, der sich ausführlich mit den Datenschutzaspekten bei den diversen smarten Geräten, die das Internet der Dinge ausmachen, beschäftigt. Laut aktuellen Untersuchungen von Cisco sind Anfang 2014 mindestens 10 Milliarden Geräte regelmäßig mit dem Internet verbunden gewesen. Momentan ist weltweit im Wesentlichen noch das IPv4 Protokoll im Einsatz, dieses ist auf 4.294.967.296 verfügbare IP-Adressen beschränkt. Ein Problem, welches nur durch technische Klimmzüge zu beheben ist. Deswegen wurde schon vor Jahren das IPv6 Protokoll entwickelt. Hier kann jedes Sandkorn dieser Erde theoretisch Milliarden IP-Adressen zugewiesen bekommen. Aber wo bleibt da der Datenschutz? Der dritte Artikel zum Schwerpunktthema beleuchtet die datenschutztechnischen Vor- und Nachteile des IPv6 Protokolls.

Natürlich haben wir auch in dieser Ausgabe wieder Datenschutznachrichten und wir weisen noch einmal auf den Kirchensteuersperrvermerk hin.

Frank Spaeing

## Autorinnen und Autoren dieser Ausgabe:

**Franziska Facius**
arbeitet als Rechtsanwältin. Bloggt über Recht und Unrecht im Netz.
facius@netzrecht-blog.de

**Dr. Safuat Hamdy**
arbeitet als Security Consultant bei der Secorvo Security Consulting GmbH in Karlsruhe.
safuat.hamdy@secorvo.de

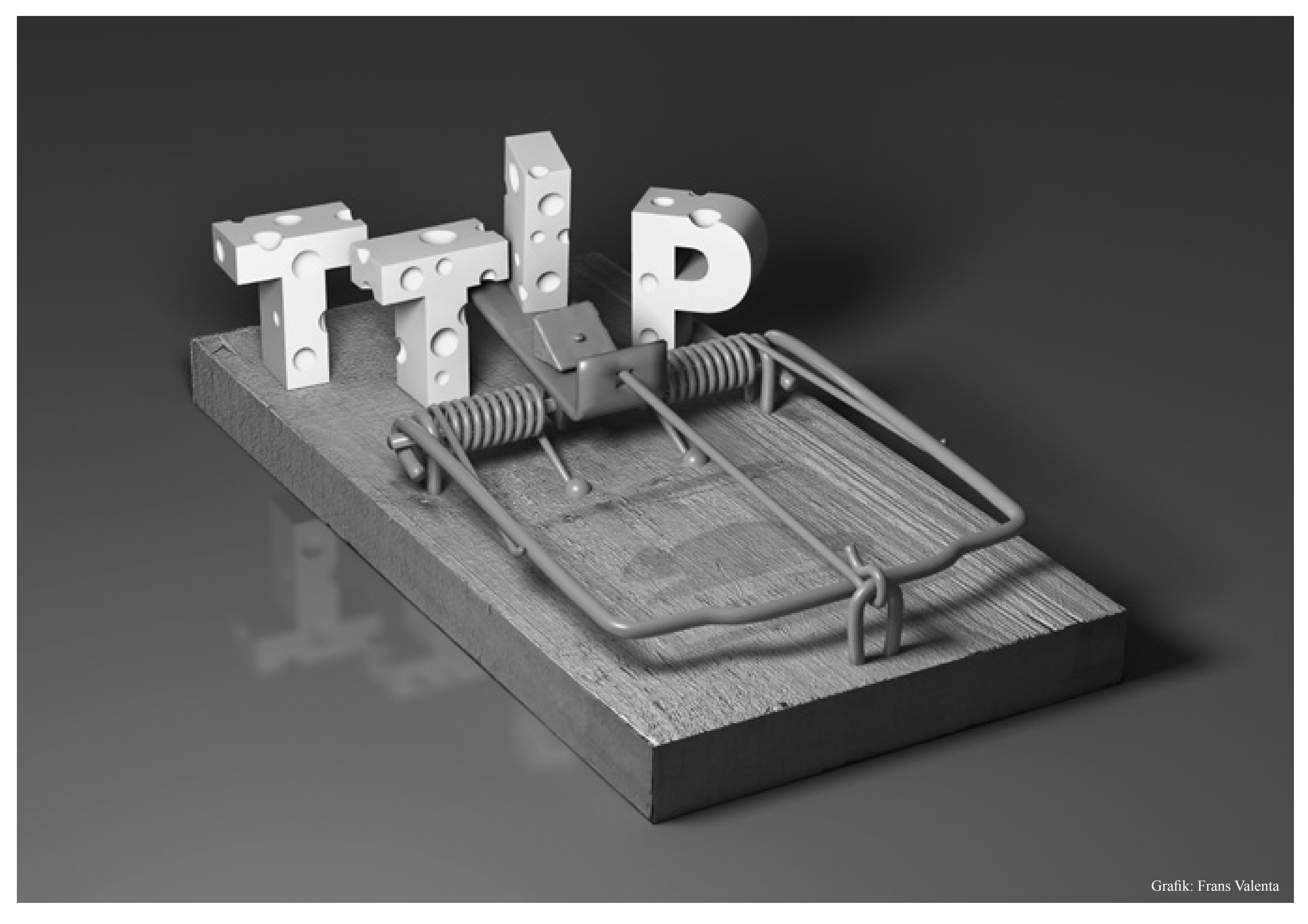
**Björn Malinka,**
Consultant für Datenschutz bei der 2B Advice GmbH,
bjoern.malinka@2b-advice.com

**Jaqueline Rüdiger**
Mitglied im Vorstand der Deutschen Vereinigung für Datenschutz e.V.
mail@jaqueline-streubel.de

**Dr. Thilo Weichert**
Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig Holstein, Kiel,
weichert@datenschutzzentrum.de

Jaqueline Rüdiger

# TTIP – Freier Handel, unfreie Bürger?




Grafik: Frans Valenta

TTIP – das steht für Transatlantic Trade and Investment Partnership, zu Deutsch: Transatlantische Handels- und Investitionspartnerschaft. Hierbei handelt es sich um ein Freihandelsabkommen, das derzeit zwischen der EU und den USA verhandelt wird. Dabei ist es nur eines von vielen. Weltweit sind 110 Länder daran beteiligt, 22 regionale Freihandelsabkommen voranzutreiben. Sowohl die USA als auch die EU verhandeln parallel mit vielen anderen Ländern. Die Gespräche zwischen diesen Beiden haben aber eine besondere Qualität, denn hier verhandeln die beiden wichtigsten Wirtschaftsräume der Welt miteinander (44 % der globalen Wirtschaftsleistung und 60 % der ausländischen Direktinvestitionen). Die Befürworter von TTIP versprechen sich Wirtschaftswachstum auf beiden Seiten des Atlantiks. Sie wollen eine mächtige Handelsunion schaffen, gegen die über Jahrzehnte kein anderes Land konkurrieren kann. Es sollen internationale Standards gesetzt werden - auch in Sachen Umweltschutz, Verbraucherschutz, Arbeitnehmerrechte und Schutz des geistigen Eigentums.

## Wachsende Kritik an TTIP

Die behaupteten positiven Effekte werden allerdings von immer mehr Kritikern – unter ihnen auch Handelsexperten und Gewerkschaften - infrage gestellt. Um diese zu erreichen, sollen durch TTIP Handelshemmnisse abgeschafft werden, sowohl tarifäre als auch nicht-tarifäre. Unter Abschaffung nicht-tarifärer Handelshemmnisse ist die Angleichung unterschiedlicher Produktvorschriften zu verstehen, die den transatlantischen Güteraustausch behindern. Von vielen Bürgern, Nichtregierungsorganisationen (NGOs) und Gewerkschaften – auf beiden Seiten des Atlantiks – sowie von einigen Politikern (Grüne, Linke, Piraten, teilweise SPD) wird daher eine Absenkung der regionalen Standards im Umwelt- und Verbraucherschutz oder von Arbeitsnormen befürchtet. Auch das hohe europäische Datenschutzniveau steht aus Sicht der Kritiker auf dem Spiel.

## Geheimniskrämerei

Die EU-Kommission und das US-Handelsministerium verhandeln TTIP

im Geheimen. Die kritischen Punkte des Abkommens sind nur deshalb bekannt, weil einzelne Passagen, Verhandlungsprotokolle u. Ä. durch Insider öffentlich gemacht wurden. Während die Öffentlichkeit ausgeschlossen wird, werden Unternehmensverbände großzügig informiert. Sie haben die Möglichkeit, direkten Einfluss auf das Abkommen zu nehmen und nutzen diese auch. Die Brüsseler NGO „Corporate Europe Observatory" zählte von Januar 2012 bis April 2014 mindestens 119 Treffen mit Konzernvertretern. Verbraucherschutz- und Umweltverbände wurden in dieser Zeit nur elf Mal gehört. Auf öffentlichen Druck gibt es nunmehr eine Beratergruppe, die sog. TTIP Advisory Group, der Vertreter von NGOs, Gewerkschaften und Wirtschaft angehören. Trotz dieser Anhörungen bleibt das Grundproblem von TTIP, dass es keine wirkliche demokratische Mitsprache und Kontrolle gibt. Das EU-Parlament kann das verhandelte Abkommen nur als Ganzes annehmen oder ablehnen. Einzelklauseln können nicht beanstandet werden. Und sobald die Vereinbarung abgeschlossen ist, lässt sie sich faktisch nicht mehr ändern, da alle Vertragspartner zustimmen müssten.

## Schiedsgerichte – noch mehr Geheimnisse

Eine Gefahr für regionale Standards stellen vor allem die Sonderrechte für Investoren dar, die ein wesentlicher Bestandteil von TTIP sind. Nicht nur der grenzüberschreitende Austausch von Waren sondern auch Direktinvestitionen im Ausland sollen durch sog. Investitionsschutzklauseln geschützt werden. Auch diese sind nicht neu. Deutschland hat bereits 130 bilaterale Verträge geschlossen, die solche Klauseln enthalten (z. B. das EU-Südkorea Handelsabkommen von 2010). Regelungen zum Investitionsschutz erlauben es ausländischen Firmen, gegen einen Staat zu klagen, wenn dieser ihre Investitionen gefährdet. Es reicht ein vermuteter Gewinnausfall aufgrund geänderter Gesetze, wenn diese den Investor direkt oder indirekt enteignen oder ihm willkürlich bzw. diskriminierend scheinen. Die Unternehmen sollen internationale Schiedsgerichte anrufen dürfen. Derartige Gerichte stehen jedoch in der Kritik, da die Öffentlichkeit von den Verfahren ausgeschlossen ist. Auch ist eine Berufung ausgeschlossen, d. h. ein einmal gefälltes Urteil ist endgültig. In den letzten Jahren mehren sich Investorenklagen. Die UN-Organisation UNCTAD berichtet, dass 54 der seit den 90er Jahren insgesamt eingereichten 514 Investorenklagen allein im Jahre 2012 eingereicht wurden. Laut UNCTAD fehlt allerdings ein genauer Überblick, da es kein offizielles Register gibt. In der Mehrzahl der Fälle gewinnen die Unternehmen oder es wird ein Vergleich geschlossen. Es sind sogar Fälle bekannt, in denen eine Investorenklage und die Rücknahme von Gesetzesentwürfen in engem zeitlichem Zusammenhang stehen. Zum Beispiel lockerte die Stadt Hamburg ihre Umweltauflagen wieder, nachdem sie von Vattenfall wegen zu strenger Vorschriften verklagt worden war und sich außergerichtlich mit dem Energieversorger geeinigt hatte. Auch bei einer Anhebung datenschutzrechtlicher Standards wären also solche Investorenklagen nach Abschluss des Abkommens denkbar und der Datenschutz möglicherweise in Gefahr.

## Die TTIP-Befürworter und die Datenschutz-Frage

Aufgrund der wachsenden öffentlichen Kritik wird die EU-Kommission nicht müde zu versichern, dass die Absenkung von Standards nicht Ziel des Abkommens sei. Insbesondere habe die EU-Kommission gar kein Verhandlungsmandat in Datenschutz-Fragen. Das bestehende Datenschutzniveau werde nicht angetastet. EU-Handelskommissar De Gucht beteuert, dass „kein europäischer Schutzstandard auf Grund dieses Freihandelsabkommens aufgegeben wird: Das gilt sowohl für Nahrungsmittel, Sozialstandards als auch für den Datenschutz. Ich werde dafür sorgen, dass TTIP nicht zu einem Dumping-Abkommen wird."

Unbeeindruckt von dem fehlenden Verhandlungsmandat der EU-Kommission in Sachen Datenschutz versuchen die USA und Unternehmen, Datenschutzfragen in den TTIP-Verhandlungen zu platzieren. Die Brüsseler NGO „Corporate Europe Observatory" hat auf Grundlage der Informationsfreiheitsrechte von der EU-Kommission Dokumente angefordert. Aus diesen zwischen Oktober 2014 und Januar 2014 veröffentlichten Dokumenten geht hervor, dass sowohl die US-Handelskammer als auch europäische und US-Unternehmen den Datenschutz in das Abkommen aufgenommen haben wollen.

Aus Sicht der Amerikaner stellt das europäische Datenschutzrecht ein Handelshemmnis dar. Aus dem Protokoll eines Gesprächs mit einem Vertreter der US-Handelskammer vom 19. April 2013 geht hervor, dass die USA ein großes Interesse daran haben, den grenzüberschreitenden Datenverkehr in TTIP zu regeln. Auch der US-Handelskommissar Froman bezeichnete nationale Speicherstrategien wie z. B. die europäische Cloud der Deutschen Telekom als „kontraproduktiv", wenn man Teil einer innovativen Wirtschaft sein wolle. „Die Menschen werden schnell bemerken, dass die Unternehmen selbst mit diesem Ansatz Probleme haben. Wenn man wirklich Innovationen schaffen will, benötigt man ein offenes Internet, mit freiem Datenfluss.", behauptete er im ARD-Interview am 04. Mai 2014.

Bei einer Anhörung der grünen Fraktion am 5. März 2014 wurde das Verhältnis zwischen EU-Datenschutz und TTIP diskutiert. Ein Vertreter der EU-Kommission betonte, die EU-Kommission habe keinen Vorschlag zu Datenflüssen eingebracht. Allerdings hätten die USA dies getan. Der Text befindet sich im E-Commerce-Chapter des Abkommens und betrifft zwei Themen. Zum einen sollen Datenströme zwischen der EU und den USA nach dem Vorbild eines Abkommens mit Südkorea geregelt werden: Die Parteien sollen bestrebt sein, es zu unterlassen, unnötige Schranken für den elektronischen grenzüberschreitenden Datenverkehr einzuführen oder beizubehalten. Zum anderen soll den Parteien verboten werden, lokale Speicherstrategien umzusetzen. Dies würde z. B. bedeuten, dass die Forderung europäischer Gerichte, europäische Vorratsdaten ausschließlich auf europäischen Servern zu speichern, mit dem Abkommen nicht vereinbar wäre. Die Kommission hat den Vorschlag bislang nicht kommentiert, will ihn jedoch analysieren.

### Was erwartet uns nun wirklich?

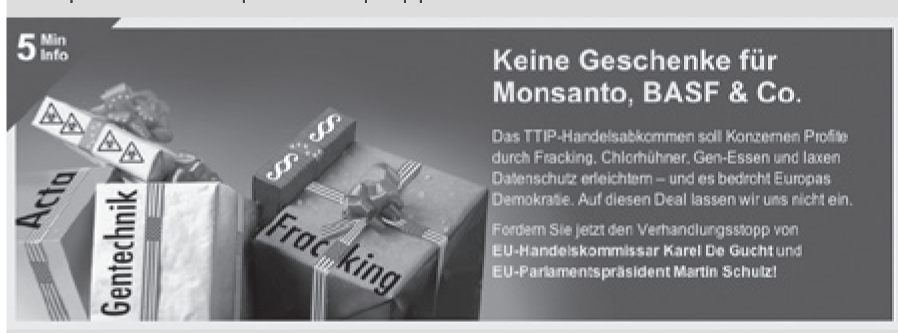
Angesichts der zunehmenden öffentlichen Kritik, stellt sich die Frage, ob eine Absenkung von Standards tatsächlich Teil des Abkommens sein wird. In diesem Zusammenhang geht z. B. die Rosa-Luxemburg-Stiftung davon aus, dass die EU-Kommission wenig Angriffsfläche bieten wird. Sie werde den Status Quo wahren, um den Kritikern die Argumente zu nehmen. Corporate Europe Observatory rechnet damit, dass sich USA und EU zunächst nur auf Standards einigen, die wenig Verhandlungsaufwand erfordern, weil sie auf beiden Seiten des Atlantiks sowieso ähnlich sind. Die prinzipielle Bedrohung von TTIP sei vielmehr, dass es als „living agreement“ ausgestaltet werden könnte. Ein solches Agreement sieht vor, dass bei jedem neuen Gesetz frühzeitig geprüft werden muss, ob es einen wesentlichen Einfluss auf den freien Handel hätte. Derartige Klauseln würden es Unternehmen in allen beteiligten Staaten ermöglichen, ihre Lobbyarbeit beträchtlich auszuweiten, da sie auf beiden Kontinenten bei der Gesetzgebung einbezogen werden müssten. Hierbei sei an die regelrechte Lobbyschlacht erinnert, die Unternehmen angesichts der neuen EU-Datenschutzgrundverordnung begonnen haben. Diesen Marktteilnehmern noch mehr Macht einzuräumen, erscheint daher nicht erstrebenswert.

Derzeit ist schwer abzusehen, welche Auswirkungen TTIP auf den Datenschutz haben wird. Sicher ist jedoch: Wenn die EU-Kommission nicht nachdrücklicher als bisher ihre öffentlich beteuerte Haltung einnimmt, dann wird das Abkommen auch Auswirkungen auf den Datenschutz haben. Vielleicht nicht sofort mit dem Abschluss; möglicherweise jedoch in einigen Jahren, wenn neue Gesetze zum Schutz personenbezogener Daten auf den Weg gebracht werden sollen. In jeder Hinsicht lohnt es sich daher, aufmerksam zu beobachten, wie sich TTIP-Verhandlungen auf den Datenschutz auswirken könnten. Besonders problematisch ist in diesem Zusammenhang, dass die Verhandlungen geheim sind und wohl bis zuletzt geheim bleiben werden. Wenn das Parlament am Ende nur zwischen Ja und Nein wählen kann, muss möglicherweise die eine oder andere unerwünschte Klausel zugunsten des Gesamtwerks akzeptiert werden. Es ist daher verständlich, dass immer mehr Menschen und Organisationen TTIP grundsätzlich ablehnen.

Quellen:
Tina Hassel, US-Handelsbeauftragter Froman im ARD-Interview „Mit TTIP hohe Standards setzen“, www.tagesschau.de, 04.05.2014; Silvia Liebrich, EU-Parlament winkt Sonderrechte für Großkonzerne durch, www.sueddeutsche.de, 01. Mai 2014; Christopher Ziedler, Wo stehen die Verhandlungen um TTIP?, www.tagesspiegel.de, 01.05.2014; Nationale Parlamente ausschalten, www.taz.de, 29.04.2014; Ulrike Herrmann, Freihandel Projekt der Mächtigen, Rosa-Luxemburg-Stiftung Büro Brüssel, April 2014; Deutscher Bundestag, Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten […] und der Fraktion DIE LINKE: EU-USA-Freihandelsabkommen und Datenschutz, Drucksache 18/1056, 07.04.2014; Katharina Nocun, Neue TTIP-Dokumente: US-Regierung und Unternehmen wollen Datenschutz umgehen, www.blog.campact.de, 11.03.2014

Ein Aufruf, den die DVD unterstützt und dem wir uns anschließen:

https://www.campact.de/ttip/appell/teilnehmen/




**TTIP: Verkauft nicht unsere Zukunft!**

Das geplante Freihandels-Abkommen TTIP zwischen der EU und den USA dient den Interessen der Konzerne und nicht uns Bürger/innen:

- TTIP höhlt Demokratie und Rechtsstaat aus: Ausländische Konzerne können Staaten künftig vor nicht öffentlich tagenden Schiedsgerichten auf hohe Schadenersatzzahlungen verklagen, wenn sie Gesetze verabschieden, die ihre Gewinne schmälern.
- TTIP öffnet Privatisierungen Tür und Tor: Das Abkommen soll es Konzernen erleichtern, auf Kosten der Allgemeinheit Profite bei Wasserversorgung, Gesundheit und Bildung zu machen.
- TTIP gefährdet unsere Gesundheit: Was in den USA erlaubt ist, würde auch in der EU legal – so wäre der Weg frei für Fracking, Gen-Essen und Hormonfleisch. Die bäuerliche Landwirtschaft wird geschwächt und die Agrarindustrie erhält noch mehr Macht.
- TTIP untergräbt die Freiheit: Es droht noch umfassendere Überwachung und Gängelung von Internetnutzern. Exzessive Urheberrechte erschweren den Zugang zu Kultur, Bildung und Wissenschaft.
- TTIP ist praktisch unumkehrbar: Einmal beschlossen, sind die Verträge für gewählte Politiker nicht mehr zu ändern. Denn bei jeder Änderung müssen alle Vertragspartner zustimmen. Deutschland allein könnte aus dem Vertrag auch nicht aussteigen, da die EU den Vertrag abschließt.

Daher fordere ich: Beenden Sie die Verhandlungen über das TTIP-Abkommen!

(Name und Ort werden angehängt)



Franziska Facius

# Das Internet der Dinge ist eine Herkulesaufgabe für den Datenschutz

Die Entwicklung des Internets und die Verknüpfung mit der analogen Welt nehmen rasant Fahrt auf. Waren vor einigen Jahren Kühlschränke, die automatisch Einkauflisten erstellen und Einkäufe erledigen, im interaktiven Haus noch Zukunftsvisionen, sind diese bereits jetzt im Handel erhältlich. Auch die Telematik in Autos ist bereits immens fortgeschritten und nur ein weiteres Beispiel für die zunehmende Vernetzung von Alltagsgegenständen mit dem Internet. Natürlich sind diese intelligenten Objekte alle smart. Es gibt das Smart-Phone, den Smart-TV und das Smart-Board. Diese Begriffe haben es auch schon in den Duden geschafft. Dort wird der Begriff smart erklärt als 1.) clever, gewitzt oder 2.) von modisch auffallender und erlesener Eleganz; fein. Auf die smarten Gerätschaften, die mit dem Internet in einer ständigen Beziehung stehen, soll eher die erste Umschreibung zutreffen.

Der Duden schreibt weiter zur Herkunft des Wortes Smart-TV: „Herkunft: aus englisch smart = mit künstlicher Intelligenz arbeitend". Nun sind diese mit künstlicher Intelligenz ausgestatteten Geräte zuweilen auch recht schlitzohrig und wenden sich von dem Nutzer ab und hin zur dunklen Seite. Wenn so ein modisch auffallendes Gerät von erlesener Eleganz seine Hüllen fallen lässt, erscheint vor dem Betrachter eine Datenkrake, die jedwedes Verhalten ihres Nutzers aufzeichnet und zur Analyse an den großen Bruder schickt.

## Der schnüffelnde Flimmerkasten – Datenschutz als Testbild

Das Smart-TV ist eine solche Datenkrake. Er hat sich auch der Passion der Datensammlung verschrieben. Dem Nutzer zeigt es sein wahres Ich nicht, sondern sammelt im Verborgenen. Heimlich öffnet es die Hintertür für Gäste und lädt zur Datenparty.

Erste Berichte über das schnüffelnde Smart-TV erschienen im Sommer letzten Jahres, als Marco Ghiglieri, Florian Oswald und Erik Tews von der TU Darmstadt ihre Arbeit mit dem Titel " HbbTV – I Know What You Are Watching" auf dem 13. Deutschen IT-Sicherheitskongress des BSI veröffentlichten.[1] Die Autoren untersuchen die Anwendung des HbbTV und kommen für den Datenschutz zu einem äußerst unbefriedigenden Ergebnis. HbbTV, welches das Internet und den DVB-Empfang auf dem Fernseher kombiniert, ermöglicht es den Sendeanstalten, nicht nur Zusatzleistungen anzubieten, sondern auch das Nutzerverhalten ihrer Zuschauer zu analysieren.[2] Ein weiteres Problem sei, so die Forscher, dass auch Dritte das Nutzerverhalten ohne Kooperation des Zuschauers oder der TV-Sender aufzeichnen können, wenn der Nutzer WLAN verwendet und dass dies auch selbst dann möglich ist, wenn das WLAN mit WPA2 abgesichert wurde.[3]

Im Verlauf des letzten Jahres mehrten sich die Berichte über Smart-TVs, die das Fernsehverhalten ihrer Nutzer ausspähen. Ein britischer IT-Experte berichtete auf seinem Blog im November 2013, dass sein Fernseher über sein Nutzerverhalten Daten sammelt und verschickt, obwohl er laut Einstellung den Datentransfer ausgeschaltet hatte.[4] Als die Zeitschrift c`t im Januar 2014 die smarten Fernsehgeräte untersuchte, konnte nur der dringende Rat gegeben werden, die HbbTV-Funktion aus Datenschutzgründen abzuschalten.[5] Ob aber bei jedem Gerät allein das Abschalten dieser Zusatzfunktion des Fernsehers genügt, um den Datenschutz zu gewährleisten, ist nicht sicher, denn nicht nur diese Funktion des Smart-TVs kann zum Datensammeln verwendet werden.

Die Stiftung Warentest hat Smart-TVs in Bezug auf den Datenschutz getestet und rät dringend dazu, bestimmte Funktionen nicht zu nutzen. In dem am 24.04.2014 veröffentlichen Beitrag: „Smart TV und Datenschutz: Spion im Wohnzimmer – wenn der Fernseher zurückschaut"[6] warnt die Stiftung nicht nur vor der HbbTV-Funktion, sondern auch vor der Nutzung von Gesichts- und Stimmerkennung, die bereits von einigen Geräten angeboten wird. Nicht nur, dass das Nutzerverhalten dann einer bestimmten Person zugeordnet werden kann, auch die biometrischen Daten der Stimmerkennung werden durch das Netz geschickt. Dies erscheint nicht nur der Stiftung äußerst bedenklich.

Sowohl die Hersteller als auch die Fernsehsender haben sich zu diesem datenschutzrechtlichen Problem verständlicherweise überwiegend nicht geäußert.

## Das Wahrnehmungsproblem

Das Internet der Dinge eröffnet die Möglichkeit der Verknüpfung des Internets mit täglichen Gebrauchsgegenständen. Dieser Fortschritt wird bereits jetzt durch die Konsumenten genutzt. Die mit der Nutzung verbundenen Risiken werden jedoch häufig nicht richtig oder gar nicht wahrgenommen. Oft ist dies auch gar nicht möglich.

Zum einen führt die Steigerung der Lebensqualität durch das Internet der Dinge im Alltag dazu, dass datenschutzrechtliche Bedenken nicht erhoben oder ausgeblendet werden. Zum anderen lassen die Geräte selbst eine genaue Prüfung wer welche Daten aus welchen Gründen sammelt nicht zu. Die Sammlung der Daten geschieht im Hintergrund und für den Nutzer nicht wahrnehmbar. Wenn der Nutzer nicht sieht was passiert, kann er sich auch letztlich nicht selbst für seinen Datenschutz sensibilisieren.

Diese Wahrnehmungsprobleme werden durch die Bestrebungen und das Bemühen der EU und der einzelnen Staaten verschärft, den neuen Technologiemarkt zu fördern und für die Wirtschaft attraktive Standorte zu schaffen. Regulierungen zu Gunsten des Datenschutzes werden als Hemmnis gesehen und nur mit der Kneifzange angefasst. Dies bestätigt auch die aktuell schleppende Gesetzgebung der EU-Datenschutz-Grundverordnung. Die Mitgliedsstaaten ihrerseits sehen keinen Grund für eigene Gesetzgebungen, und begründen dies mit der Angst, die Harmonisierung des Rechts zu gefährden.

## Konsultation der Europäischen Kommission zum Internet der Dinge und Expertengruppe

An der durch die Europäische Kommission 2012 initiierten Befragung beteiligten sich über 600 Personen, hierunter waren unter anderem Vertreter aus der Wirtschaft, Interessensverbände, Forscher und interessierte Bürger. Die Konsultation wurde durchgeführt, um neue Richtlinien vorschlagen zu können.[7] Im Wege der Konsultation erhielt die Kommission Meinungsäußerungen zu den Themen Schutz der Privatsphäre, Sicherheit, Gefahrenabwehr, Ethik, Interoperabilität, Leitungs- und Aufsichtsmechanismen und Standards.[8]

Die Ergebnisse der Konsultation wurden im Frühjahr 2013 veröffentlicht. Die Befragten teilten zu der Problematik „Datenschutz und Geheimhaltung“ je nach der Gruppe der Befragten unterschiedliche Interessen mit. Die Vertreter der Wirtschaft erachten die derzeitig bestehenden Datenschutzregeln auch für das Internet der Dinge als ausreichend, so dass es keiner weiteren Regelungen über den Datenschutz für das Internet der Dinge bedürfe. Einige Befragte sprachen sich ausdrücklich gegen eine staatliche Intervention aus, da sie befürchten, dass hierdurch die technische Innovation erstickt werden könnte, auch würden die Anforderungen an die Erstellung von Guidelines die Wirtschaft über Gebühr beanspruchen.[9] Nach Ansicht der Vertreter der Industrie könnten dauernde und explizite Fragen nach datenschutzrechtlichen Einwilligungen die weitere Entwicklung des Internets der Dinge verhindern. Die Wirtschaft forderte in der Befragung, dass es möglich sein müsse, anonymisierte Daten mit Dritten austauschen zu können.

In Kontrast dazu stehen die mehrheitlich geäußerten Interessen der befragten Bürger und Verbraucherschutzorganisationen am Datenschutz im Zusammenhang mit dem Internet der Dinge. Nach Ansicht der befragten Bürger (77%) ist der jetzige Datenschutz für Anwendungen des Internets der Dinge nicht effizient und eine Fokussierung auf Geheimhaltung und Datenschutz dringend notwendig. Im Einzelnen wurden durch die Befragten folgende Grundsätze unterstützt:

- Der Grundsatz des Zustimmungsvorbehalts des Nutzers bei Datenerhebungen. Der Nutzer selbst soll entscheiden, ob er Teil eines Internet-der-Dinge-Systems wird oder nicht.
- Persönliche Daten sollen nicht ohne die ausdrückliche Einwilligung des Nutzers erhoben werden dürfen. Eine Datenschutzorganisation warnte davor, dass aufgrund der automatischen Kommunikation zwischen den vernetzten Geräten ausufernde Personenprofile erstellt werden können und erläuterte, dass dieses Phänomen heute schon in der üblichen Internetumwelt vorliegt.
- Technischer Datenschutz durch Anonymisierung der Daten wird von den Befragten als sehr wichtig angesehen.
- Transparenz muss garantiert sein, so dass der Nutzer darüber zu informieren ist, wann, wie, weshalb und auf welchem Weg persönliche Daten von ihm erhoben werden.
- Datenschutz durch Technik (Privacy by Design) und datenschutzfreundliche Voreinstellungen (Privacy by Default) müssen umgesetzt werden.
- Um illegalen Zugriff auf die Geräte zu vermeiden, sollte die Systemsicherheit inklusive Verschlüsselungstechniken oberste Priorität haben.
- Die Einwilligung zur Datenerhebung sollte zeitlich begrenzt und jederzeit widerruflich sein.
- Faire und gerechte Prinzipien werden von den Befragten gefordert.
- Einige Befragte forderten für den Datenschutz von unabhängigen Stellen erstellte Audits.[10]

Die von der Europäischen Kommission eingesetzte Expertengruppe kommt in ihrer Faktensammlung „Datenschutz und Sicherheit bei dem Internet der Dinge“ unter anderem zu dem Ergebnis:

“It should be ensured, that individuals remain in control of their personal data and that IoT systems provide sufficient transparency to enable individuals to effectively exercise their data subject rights. This also involves, that in cases where data processing takes place based on consent, a clear and non-discriminative choice must exist to refuse consent. Furthermore it should be clarified, under which circumstances the consent of individuals to certain data processing activities should be considered to be valid. Especially in the case of IoT, individuals will often lack the necessary understanding of the technical functioning and therefore of the consequences of their consent. Clear rules on the conditions that need to be met for consent to be valid, should be defined.”[11]

## Keine technische und rechtliche Sicherheit für den Datenschutz

Weder für den Datenschutz noch für den normalen bürgerlich rechtlichen Vertrag im Zusammenhang mit intelligenten Geräten gibt es derzeit einen klaren gesetzlichen Rahmen in Deutschland.

Mit der Frage, welche Rechte der Verbraucher hat, wenn intelligente Geräte mangelhaft sind, haben sich Christian Solmecke und Simon-Elias Vondrlik in ihrem Beitrag: „Rechtliche Probleme bei Produkten mit serverbasierten Zusatzdiensten. Was passiert, „wenn der Kühlschrank keine Einkaufsliste mehr schreibt...” befasst.[12] Die Autoren kommen zu dem Ergebnis, dass es sich bei dem Vertrag über den Kauf eines intelligent vernetzten Kühlschranks nicht nur um einen reinen Kaufvertrag handelt, sondern in Bezug auf das Angebot von serverbasierten Zusatzdiensten ein dauerhafter Dienstvertrag vorliegt.[13] In dem Fazit führen die Autoren zutreffend aus: „Insgesamt ist der Branche dringend zu empfehlen, die Rechtslage zu analysieren und die Rechte und Pflichten der Beteiligten vertraglich zu regeln“.[14]

Weitere rechtliche Probleme ergeben sich aus der Nutzung der sog. Firmware. Bei Firmware handelt es sich um eine durch den Hersteller in die Geräte implementierte Software, ohne die das Gerät nicht betrieben werden kann. Die in die Geräte implementierte Software hat oft auch Open-Source-Komponenten. Oftmals ist nicht klar abzugrenzen, welcher Teil der Firmware die Sicherheitslücke verursacht, welche Gefahren durch diese drohen und welcher Schaden entstehen kann. Die Haftungsfragen bei mangelhafter Firmware sind äußerst facettenreich, rechtlich nicht abschließend geklärt und haben auch für den technischen Datenschutz eine große Bedeutung.

Dass die Firmware oft mangelhaft ist und „Datenlecks" hat, zeigt jüngst die Aufregung um Hintertüren in Routern. Wenn Hacker über einen gekaperten Router teure Telefonate abhalten können, dann ist es für denjenigen, der Daten sammeln will, ebenso möglich, diese direkt beim Erzeugen illegal zu erheben, ohne dass dies bemerkt wird. Die Gefahr einer solchen Datensammlung besteht grundsätzlich bei allen intelligent vernetzten Geräten, da auch diese nur mit einer sog. Firmware funktionieren.

Zu der Problematik der Firmware bei Routern schrieb Heise online: „Angesichts der immer häufiger auftretenden Sicherheitsprobleme mit Router-Firmware stellt sich die Frage, ob Hersteller nicht über neue Update-Mechanismen nachdenken sollten. Aktuelle Ansätze scheinen nicht mehr auszureichen, um die Sicherheit von Nutzern zu gewährleisten."[15]

## Technische Standards und rechtlicher Rahmen müssen schnellsten geschaffen werden

Derzeit gibt es keine einheitlichen technischen Standards für intelligent vernetzte Geräte. Die Hersteller haben auch für die Umsetzung des technischen Datenschutzes keine Vorgaben. Viele Hersteller blenden den Datenschutz aus.

Datenhändler und Cyberkriminelle werden bereits Wege gefunden haben, vernetzte Geräte für sich auszunutzen. Oft werden die Angriffe auf die intelligenten Geräte sogar verborgen bleiben, da der Verbraucher keine Möglichkeiten hat, eigene Sicherheitsvorkehrungen zu treffen und sich blind auf die Firmware verlassen muss. Dass vernetzte Geräte sich aufgrund dieser Umstände auch bei Spam-Mail Attacken als schweigsame Helfer erweisen können, beweist eine erste nachgewiesene Spam-Mail Attacke Ende 2013 und eine weitere Anfang 2014. Die Mehrheit der an dieser Attacke beteiligten Geräte waren vernetzte Geräte wie beispielsweise Multimedia Center, Fernseher und sogar ein Kühlschrank.[16]

Die bestehenden nationalen und europäischen Datenschutznormen sind unzureichend für eine Anwendung auf das Internet der Dinge. Die Datenschutz-Grundverordnung der EU wird erst in weiter Zukunft in Kraft treten. Die Besonderheiten für den Datenschutz bestehen beispielsweise in der Vielzahl der Nutzer eines intelligenten Gerätes in einem Haushalt. Die Einwilligung muss von jeder dieser Personen vorliegen. Es ist nicht geklärt, wie der Nutzer seine Einwilligung zur Datenerhebung durch ein intelligent vernetztes Gerät wirksam abgibt und welche Anforderungen notwendig sind, wenn eine dauernde Datenüberwachung durch das Gerät erfolgt. Ein weiteres Problem liegt bei den Geräten selbst, da die überwiegende Zahl der intelligenten Geräte unterschiedliche Daten weltweit an verschiedene Stellen verschickt.

## Blauäugig ist die EU nicht, aber im Verzug

Blauäugig ist die EU in Bezug auf das Internet der Dinge und den Datenschutz sowie die Wahrung des informationellen Selbstbestimmungsrechts tatsächlich nicht, dies beweist die Arbeit der Kommission und der einberufenen Expertengruppe.

Leider wird die Technik den Markt schon längst für sich erobert haben, bevor überhaupt nur eine Richtlinie in dieser Hinsicht auf EU-Ebene besprochen wird. Dann wird es schwer, wenn nicht unmöglich sein, die Standards verbindlich und allumfassend nachzurüsten. Das ist ein beträchtlicher Verzugsschaden für Datenschutz und Persönlichkeitsrecht.

1 http://www.cased.de/files/2013_CASED_HbbTV.pdf.

2 http://www.cased.de/files/2013_CASED_HbbTV.pdf, S. 1.

3 http://www.cased.de/files/2013_CASED_HbbTV.pdf, S. 9 f.

4 http://doctorbeet.blogspot.co.uk/2013/11/lg-smart-tvs-logging-usb-filenames-and.html.

5 http://www.heise.de/newsticker/meldung/Spion-im-Wohnzimmer-c-t-ertappt-schnueffelnde-Fernseher-2096578.html .

6 https://www.test.de/Smart-TV-und-Datenschutz-Spion-im-Wohnzimmer-wenn-der-Fernseher-zurueckschaut-4695977-0/

7 Pressemitteilung der Europäischen Kommission vom 12.04.2012: Digitale Agenda: Kommission veranstaltet Konsultation zu Regeln für vernetzte intelligente Geräte – das „Internet der Dinge"; http://europa.eu/rapid/press-release_IP-12-360_de.htm

8 s.o.

9 Report on the public consultation on IoT Governance, S.4; http://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation

10 Report on the public consultation on IoT Governance, S.4; http://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation

11 Internet of Things Factsheet Privacy and Security, IoT Privacy, Data Protection, Information Security, S.7; http://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation

12 Solmecke/Vondrlik: Rechtliche Probleme bei Produkten mit serverbasierten Zusatzdiensten – Was passiert, „wenn der Kühlschrank keine Einkaufsliste mehr schreibt ..."; MMR 2013, 755 ff.

13 Solmecke/Vondrlik, MMR 2013, 755, 757.

14 Solmecke/Vondrlik, MMR 2013, 755, 758.

15 Heise online am 05.02.2014 12:29; #Asusgate: Zehntausende Router geben private Dateien preis, http://www.heise.de/newsticker/meldung/Asusgate-Zehntausende-Router-geben-private-Dateien-preis-2105778.html

16 t3n.de am 20.01.2014 15:46; Botnet: Zombie-Kühlschränke versenden 750.000 Spam-Mails, http://t3n.de/news/botnet-kuehlschraenke-fernseher-523254/

Björn Malinka

# Smart Meters: Zusammenfassung von Messdaten kann für Energieversorger ausreichend sein

Die beschlossene Energiewende sieht den Handlungsbedarf nicht ausschließlich auf Seiten der Energieversorgungsunternehmen (EVU). Vielmehr sollen auch die Konsumenten in die Pflicht genommen werden, die verfügbare Energie bewusster und effizienter zu nutzen. In diesem Kontext kommt intelligenten Zählern, sogenannten Smart Meters, eine immer bedeutendere Rolle zu. Sie bieten für private Haushalte ebenso wie für Gewerbetreibende eine Fülle von Informationsmöglichkeiten über den aktuellen Energieverbrauch. Mithilfe eines Smart Meters kann rund um die Uhr der aktuelle Energieverbrauch kontrolliert werden. Dies hilft, den eigenen Verbrauch besser zu steuern und konkrete Einsparmöglichkeiten zu identifizieren. Der intelligente Zähler führt dabei nicht direkt zu Energieeinsparungen. Er liefert Letztverbrauchern, Netzbetreibern und Erzeugern lediglich die für das Lastenmanagement notwendigen Verbrauchsinformationen.

## Bedarfsgerechte Planung der Netzauslastung

Das Ziel einer möglichst zuverlässigen und gleichzeitig kostengünstigen Energieversorgung verlangt eine möglichst bedarfsgerechte Planung der erforderlichen Energieeinspeisung und Netzauslastung. Als Basis dieser Überlegungen bedienen sich EVU statistischer Daten. Die einfachste Möglichkeit für die Ermittlung der Abnahmemenge ist die Nutzung des sogenannten Standardlastprofils (SLP). Beruhend auf vergangenen Messwerten stellt es die durchschnittliche Abnahme einer bestimmten Verbrauchsgruppe dar. Dabei dient es lediglich als vereinfachte Prognose des von Tages- und Jahreszeit abhängigen Stromverbrauchs. Die tatsächliche Abnahmemenge kann von Tag zu Tag variieren, sollte jedoch nicht zu stark abweichen. Zusätzlich zum SLP werden die Auswirkungen vergangener Ereignisse auf das zukünftige Verbrauchsverhalten berücksichtigt. So wirken sich beispielsweise planbare Medienereignisse, wie die Übertragung eines Fußballfinales, aber auch spontane und unvorhersehbare Ereignisse der vergangenen Tage oder Stunden, wie beispielsweise ein unvorhergesehener Kälteeinbruch, auf das Konsumverhalten der Letztverbraucher aus.

Die Informationen über die auf der Kundenseite verbrauchten Energien werden gesammelt, ausgewertet und verarbeitet. Dies erfordert ein intelligentes Datennetz, welches parallel zum Stromnetz entsteht. Es steuert die Erzeugung, Verteilung und Speicherung von Energie mit Hilfe der erhobenen Verbrauchsdaten der Anschlussnutzer. Je nach Ausprägung dieser Informationen sehen Datenschutzexperten ein erhebliches Missbrauchspotenzial. Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD-SH) hat in diesem Zusammenhang bereits im September 2009 auf die Gefahren des kontaktlosen und unbemerkten Auslesens von Energiezählern hingewiesen.[1] Bis zum Jahr 2014 hat das Thema „Datenschutz bei Smart Metern“ an Brisanz nicht verloren – im Gegenteil. Der Europäische Datenschutzbeauftragte Peter Hustinx hat in seiner Tätigkeitsvorschau für 2014[2] angekündigt, sich des Themas „Smart Meter“ zeitnah anzunehmen. Und selbst Union und SPD haben sich im Koalitionsvertrag vom 27. November 2013 der Schaffung verlässlicher Rahmenbedingungen für den sicheren Einsatz von intelligenten Messsystemen für Verbraucher, Erzeuger und Kleinspeicher für das Jahr 2014 verschrieben. Sie streben die Schaffung hoher technischer Standards zur Gewährleistung von Datenschutz und Datensicherheit sowie Datenschutzregeln für ein intelligentes Last- und Erzeugungsmanagement an.[3] Grundlagen hierfür wurden in Deutschland bereits mit dem BSI-Schutzprofil und der zugehörigen Technischen Richtlinie gelegt.[4]

## Erhöhte Datenvolumen durch den Einsatz digitaler Zähler

Die Möglichkeit der digitalen Fernauslesung von Verbrauchsständen führt unweigerlich zu einem Anstieg der zu verarbeiteten Datenvolumen. Der bisher jährlich durchgeführte manuelle Ableseturnus erfolgt mit Einführung digitaler Smart Meter in einem 15-Minuten-Takt. Ein einziges digitales Verbrauchsmessgerät führt somit in 24 Stunden bereits 96 Messungen durch – auf ein Jahr gerechnet kommen somit über 35.000 Datensätze zusammen. Bei einem Messvorgang ermittelt der Zähler den Zählpunkt (Land, Netzbetreiber, Postleitzahl und Zählpunkt), den Zeitstempel und Zählerstand sowie weitere Informationen und gegebenenfalls die Signatur des Zählers. Insgesamt ergibt sich daraus ein Rohdatenvolumen von ca. 250 Byte.[5] Bei einem Ausleseturnus von 15 Minuten hätte beispielsweise einer der größten Energieversorger in Deutschland – mit 16,4 Millionen privaten und gewerblichen Messstellen im Strombereich – eine Datenmenge von ca. 144 Terabyte pro Jahr zu verarbeiten.

## Auswertung von Lastprofilen

In Anbetracht dieses immensen Datenaufkommens sind die Ausforschungspotenziale in diesem Zusammenhang nicht von der Hand zu weisen. Anhand der erhobenen Messdaten lassen sich Last- und Nutzungsprofile bilden, welche den häuslichen Ressourcenverbrauch widerspiegeln können und so einen Einblick

in die private Lebensgestaltung der Letztverbraucher ermöglichen.

Im folgenden Beispiel lässt die Betrachtung des dargestellten Lastprofils erkennen, dass es sich bei dem Stromverbraucher um eine Waschmaschine handelt. Die anfängliche Last von ca. 100 Watt entspricht dem Pumpvorgang zu Beginn des Waschvorgangs. Darauf folgt, mit einer Spitzenlast von durchschnittlich 2.100 Watt, die 10-minütige Aufheizphase des Wassers. Ist die notwendige Temperatur erreicht, beginnt mit durchschnittlich ca. 100 Watt das Waschen und Schleudern. Die minimalen Lastspitzen im letzten Drittel der Kurve lassen jeweils auf die Schleudervorgänge schließen.

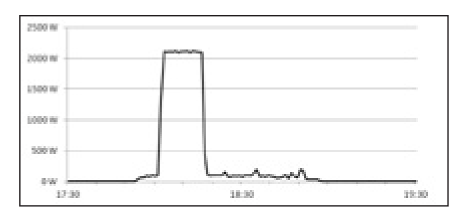



Abbildung 1: Lastprofil einer Waschmaschine (Quelle: eigene Darstellung auf Datenbasis der Technischen Universität Darmstadt)

An dieser Stelle schlummert das erste Missbrauchspotenzial. Werden die gesammelten Daten zu Werbezwecken an Dritte übermittelt, könnte beispielsweise ein Waschmaschinenhersteller anhand des Lastprofils den genauen Gerätetyp ermitteln. Stellt er fest, dass es sich um ein älteres Modell handelt, könnte er im jeweiligen Haushalt gezielte Werbeaktionen für Nachfolgemodelle starten. Riskanter wird das Thema, fasst man die Lastprofile verschiedener Haushaltsgeräte zusammen. Wie in Abbildung 2 anschaulich dargestellt, lassen sich mit der Überlagerung einzelner Lastprofile verschiedener Stromverbraucher sowie der Betrachtung des jeweiligen Stromverbrauchs und Nutzungszeitpunktes, Rückschlüsse auf die Lebensgewohnheiten der Haushaltsmitglieder vermuten. So lässt das Ausschalten des Lichtes um 0:30 Uhr beispielsweise auf die Zubettgehzeit schließen – der Peak drei Stunden später vielleicht auf einen nächtlichen Toilettenbesuch. Die Lastspitzen des Wasserboilers um 9:30 Uhr und 10:00 Uhr könnten von der zweimaligen Nutzung der Dusche herrühren – wahrscheinlich ein Anzeichen für einen Zweipersonenhaushalt. Die weitere Betrachtung der Lastprofile lässt ferner Aussagen zu Essgewohnheiten und der abendlichen Freizeitgestaltung zu.

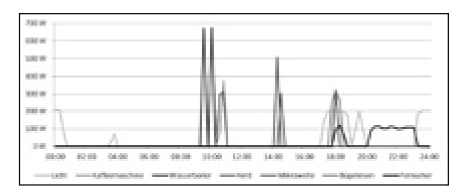


Abbildung 2: Überlagerte Lastprofile eines Haushaltes (Quelle: eigene Darstellung auf Datenbasis der Technischen Universität Darmstadt)

Noch einen Schritt weiter sind Forscher der Fachhochschule Münster gegangen. Sie haben in einem Experiment den Stromverbrauch eines TV-Gerätes analysiert, die jeweils aufeinander folgenden Helligkeitswerte gemessen und konnten auf diese Weise den Stromverbrauch des Fernsehers bestimmen. Obwohl der eingesetzte Smart Meter den Strom für den gesamten Vierpersonenhaushalt gemessen hat, also nicht direkt mit dem TV-Gerät verbunden war, konnte neben der Einschaltzeit des Fernsehers auch das eingeschaltete Programm beziehungsweise abgespielte Film identifiziert werden.[6]

## Planung der Netzauslastung – wie viele Informationen sind erforderlich?

Der Verteilnetzbetreiber (VNB) ermittelt zum Zweck des Energiemanagements sowie der Netzplanung den aktuellen Zustand des Stromversorgungsnetzes. Die hierdurch ermittelten Ergebnisse liefern ihm in erster Linie die Grundlage zur Sicherstellung der Energieversorgung sowie für weitere Entscheidungen hinsichtlich Netzkapazitäten und -ausbau. Zu diesem Zweck werden Netzzustandsdaten wie die Spannung, Frequenz, Strom und Phasenwinkel, die Geräte-ID des Zählers, die jeweiligen Messwerte, die eindeutige Zählpunktbezeichnung und viele weiteren Informationen gesammelt und im Smart Meter zum Abruf durch den VNB listenartig aufbereitet.[7]

Logischerweise plant der Energieversorger den Energiebedarf nicht individuell für jeden Haushalt – er kumuliert ihn für einen gesamten Netzabschnitt. Dies wirft die Frage auf, ob eine kumulierte Übermittlung der personenbezogenen Verbrauchsdaten nicht ausreichend ist.

Welche Auswirkung die Zusammenfassung von Verbrauchsdaten verschiedener Zähler auf die Aussagekraft der Verbrauchsverhalten hat, zeigt beispielhaft Abbildung 3.[8] Als Referenzwert dient die Lastkurve eines einzelnen Haushaltes, gemessen in einem 15-Minuten-Takt. Bemerkenswert sind dabei die hohen Ausprägungen um 7:30 Uhr, 10:15 Uhr, 17:45 Uhr sowie um 19:30 Uhr.

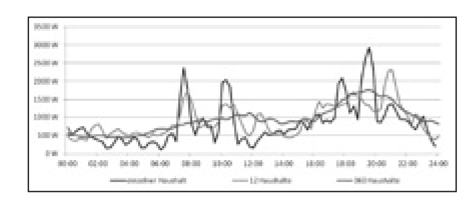


Abbildung 3: Kumulierte Verbrauchsdaten mehrerer Haushalte (Quelle: eigene Darstellung auf Datenbasis der Technischen Universität Darmstadt)

Im Vergleich zum Referenzwert lässt die Lastkurve mit 12 aggregierten Haushalten (einem Mehrfamilienhaus entsprechend) die zuvor bemerkten Ausprägungen in leicht abgeschwächter Form deutlich wiedererkennen. Eine Zustandsprognose zur Netzauslastung sollte offensichtlich weiterhin möglich sein. Die Messung der Netzauslastung an einer Transformatorenstation (auch als „Trafohäuschen“ bekannt), zeigt die Kumulierung der Messdaten aus 360 Haushalten. Auch dieses Profil lässt die Tendenzen des Stromverbrauchs erkennen.

## Fazit

Die Schaubilder zeigen, dass EVU trotz kumulierter Messdaten über mehrere Haushalte ausreichend Informationen zum Netzzustand gewinnen können. Ihr primäres Ziel, die Sicherstellung der Energieversorgung, dürfte in keinster Weise beeinträchtigt werden. Expertenmeinungen bestärken diese Annahme: „Um Netze intelligenter zu machen, reicht es aus, an bestimmten Punkten im Netz zu messen. Zum Beispiel am Trafohäuschen an der Straßenecke. Das ist sogar wesentlich effektiver.“[9] meint Gerhard Radtke, Abteilungsleiter Rollout Smart Meter, RWE Metering GmbH. Dieser Meinung schließt sich auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Düsseldorfer Kreis an: „Eine

Zuordnung zu einer Ortsnetzstation ist ausreichend. Dies kann über ein Pseudonym für eine Ortsnetzstation erreicht werden. Weiter sind Messungen an Ortsnetzstationen denkbare Alternativen."[10]

Letztendlich ist die Frage nach der Granularität der Messdaten abhängig von der Zweckbestimmung der Datenverarbeitung. Ist die Zusammenfassung von Verbrauchsdaten zum Zweck der Netzplanung auf Ebene der Ortsnetzstationen ausreichend, könnten andere Anwendungsfälle umfassendere Daten erfordern, wie beispielsweise die Rechnungslegung der EVU. Sie sind verpflichtet, jedem Kunden seine persönlichen Verbräuche in Rechnung zu stellen und gegebenenfalls transparent zu machen. Eine Verarbeitung seiner personenbezogenen Daten ist erforderlich. Dem Gutachten des ULD-SH zufolge wäre jedoch eine geringere zeitliche Auflösung eine Alternative, sofern der Kunde nicht eine anders lautende Einwilligung erklärt hat. Der Gesetzgeber hat sich zu diesem Punkt bis dato noch nicht konkret geäußert.

1 ULD-SH, Bewertung Smart Meter, 2009, https://www.datenschutzzentrum.de/smartmeter/20090925-smartmeter.html

2 EDSB, Tätigkeitsvorschau 2014, 2013, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Priorities/13-12-18_Inventory_2014_final_EN.pdf

3 Bundesregierung, Koalitionsvertrag, 2013, S. 58 ff.

4 BSI, Technische Richtlinie, https://www.bsi.bund.de/DE/Themen/SmartMeter/TechnRichtlinie/TR_node.html;jsessionid=B9C06B9A66DA095E4772B9A9C8B98779.2_cid286

5 Aichele, C., Doleski, O. D., Smart Meter Rollout, 2013., S. 311.

6 Greveler, U., Justus, B., Löhr, D., Identifikation von Videoinhalten, 2013, http://1lab.de/pub/GrJuLo_Smartmeter.pdf

7 Vgl. BSI, TR-03109-1, 2013, S. 100, Zeile 2047 i.V.m. Zeile 2051.

8 Die Darstellung wurde dabei nicht aus Lastprofilen unterschiedlicher Haushalte gewonnen, sondern tatsächlich durch die Kumulierung von Lastprofilen über mehrere Tage eines Haushaltes.

9 Radke, G., WDR, Bericht aus Brüssel, 2013, 26. Juni 2013, 22.00 - 22.15 Uhr.

10 Düsseldorfer Kreis, Orientierungshilfe datenschutzgerechtes Smart Metering, 2012, S. 38.

Safuat Hamdy

# IPv6 und Privatsphäre

Die Einführung von IPv6 hat explizit die Wiedereinführung des Ende-zu-Ende-Prinzips zum Ziel, bei dem jedes System im Internet seine eigene global routbare Adresse erhält und prinzipiell aus dem gesamten Internet angesprochen werden könnte. Dies hat in verschiedenen Diskussionsforen und Blogs sowie bei Systemadministratoren und Datenschützern zu Bedenken [DSBL 2011, Schaar 2011] wegen IPv6 geführt.

In diesem Artikel werden die relevanten Zusammenhänge zwischen IPv6 und Datenschutz dargestellt. Dabei wird der Frage nachgegangen, inwieweit IPv6 eine Bedrohung für die Privatsphäre darstellen könnte, welche Gegenmaßnahmen ergriffen werden können, und ob Privatsphäre auf diese Ebene nicht ohnehin eine Chimäre ist.

## 1 Hintergrund

IPv6 ist das Netzwerkprotokoll, das als Nachfolger für das bisher genutzte IPv4 entwickelt wurde. Die Aufgabe des Internet-Protokolls (IP) besteht im Wesentlichen darin, Datenpakete von einem System über verschiedene Netzwerke hinweg zu einem Zielsystem zu vermitteln. Diese Vermittlung erfolgt anhand von sogenannten IP-Adressen. Ohne eine gültige IP-Adresse kann ein System nicht am Internet teilnehmen.

Mit der Aufzehrung des IANA-Pools für IPv4 im Jahr 2011, in welchem IANA ihren letzten /8-Block vergeben hat, wurde ein wichtiger „Meilenstein" in dem Lebenszyklus von IPv4 erreicht. Zwar verfügen die Registrierungsstellen (RIRs) noch über freie Adressblöcke, jedoch werden auch diese Adressblöcke in absehbarer Zeit aufgezehrt sein.[1]

Diese Situation war bereits seit der enormen Expansion des Internets ab Mitte der Neunziger Jahre absehbar. Aus diesem Grund wurden seit etwa 1993 mehrere Maßnahmen ergriffen, um das Problem anzugehen. Als langfristige Maßnahme wurde eine neues Internet Protocol entworfen, das unter anderem über einen so großen Adressraum verfügen sollte, dass Engpässe bei der Adressvergabe auf absehbare Zeit unter Berücksichtigung der absehbaren Expansion des Internets nicht mehr auftreten sollten. Dieses Protokoll ist IPv6.

Als kurzfristige Maßnahme zur Linderung des Problems wurde Network Address Translation (NAT) im Zusammenspiel mit dynamischer Adressvergabe für Privatanwender eingeführt. Es gibt verschiedene Formen von NAT. Im Kontext der nachfolgenden Diskussion ist allein das One-to-Many-NAT (auch als Cone NAT bekannt) von Interesse, bei dem ein komplettes Netzwerk nach außen hin auf eine IP-Adresse abgebildet wird. Wenn in dem Netzwerk private IP-Adressen nach RFC 1918 verwendet werden, dann kann auf diese Weise der Adressraum künstlich gedehnt werden, d. h. es können mehr Systeme an das Internet angeschlossen werden als global routbare Adressen vorhanden sind.

One-to-Many-NAT hat aus Sicht der Sicherheit und des Datenschutzes einige interessante Nebenwirkungen: Erstens wirkt das System, auf dem das NAT erfolgt, quasi wie eine Firewall. Zweitens kann von außen nicht mehr anhand der IP-Adresse zwischen verschiedenen Systemen des inneren Netzes unterschieden werden.

Aus technischer Sicht werden NAT und dynamische Adressvergabe mit IPv6 obsolet. Dies führt bei Datenschützern zu Bedenken gegen IPv6, da diese Funktionen einen – zumindest subjektiv wahrgenommenen – Beitrag zur Privatsphäre der Anwender leisten.

### 1.1 IPv4-Adressen

Man unterscheidet zwischen statischen und dynamischen IP-Adressen. Statische IP-Adressen werden fest vergeben und ändern sich praktisch nie. Diese Adressen werden bei IPv4 in der Regel an Systeme vergeben, auf denen öffentlich erreichbare Dienste betrieben werden. Dynamische IP-Adressen ändern sich dagegen mehr oder weniger oft und werden in der Regel an Endkunden vergeben, die nur Clients betreiben; die überwiegende Mehrheit der Privatanwender fällt hierunter.

Der Grundgedanke bei der Vergabe dynamischer Adressen war wie bei NAT eine optimale Nutzung eines knappen Adressraumes. In der Regel sind nicht alle Privatanwender gleichzeitig online, außerdem sind Privatanwender in der Regel nicht darauf angewiesen, eine bestimmte IP-Adresse zu verwenden. Daher können momentan nicht genutzte IP-Adressen frei an andere Privatanwender vergeben werden. Dadurch erhalten Privatanwender in der Regel jeweils eine andere IP-Adresse. Diese technische Notlösung erweist sich aus Sicht des Datenschutzes als interessant, weil dadurch ein Tracking auf Grundlage der IP-Adresse schwieriger wird.

Mittlerweile sind viele Nutzer durch Angebote wie DSL oder Internet über Kabelnetze permanent online. Bei DSL kommt es in der Regel zu einer Zwangstrennung, beispielsweise nach 24 Stunden, um IP-Adressen von ungenutzten Anschlüssen wieder „einzusammeln" und neu vergeben zu können. Dies führt dann an einem DSL-Anschluss täglich zur Vergabe einer neuen IP-Adresse. Die Kabelnetz-Anbieter führen dagegen keine Zwangstrennung durch, so dass ein Anschluss für eine längere Dauer (Wochen oder Monate) dieselbe IP-Adresse haben kann.

### 1.2 IPv6-Adressen

Eine IPv6-Adresse ist 128 Bit lang und besteht aus einem 64-Bit-Präfix und einer 64-Bit Interface-ID. Der vordere Teil des Präfix wird vom Provider vorgegeben, der hintere Teil des Präfix, die Subnet-ID, wird vom Administrator oder vom Anwender vergeben. Die Interface-ID wird in der Regel vom System gewählt oder lokal per DHCPv6 zugewiesen.

Mit IPv6 ist zunächst keine dynamische Vergabe von IP-Adressen vorgesehen. Provider vergeben ihre Präfixe in der Regel statisch, da der Grund für die dynamischen Wechsel entfallen ist. Zudem markiert die Vergabe eines Präfix, etwa eines /56-Präfix, dass nicht eine einzelne Adresse sondern mehrere Netze vergeben werden. Somit entfällt auch der Grund für NAT. Daher sind sowohl Präfix als auch Interface-IDs statisch. Dies gilt aus Datenschutzsicht jedoch als problematisch.

Als besonders bedenklich erweist sich die ursprüngliche Konstruktion der Interface-ID aus der Hardware-Adresse, also etwa der MAC-Adresse. Dieser sogenannte EUI-64-Identifier ermöglicht es einem Beobachter, allein aus der IPv6-Adresse auf die verwendete Hardware des Clients zu schließen. Die Motivation für diese Konstruktion war, auf möglichst einfachem Weg eine eindeutige Interface-ID zu erzeugen. Unter Windows 7 und nachfolgend wird davon abgewichen und eine pseudozufällige Interface-ID erzeugt, die jedoch ebenfalls statisch ist.

- Um den Effekt einer dynamischen IPv6-Adresse wie bei IPv4 zu bekommen, muss erstens das Präfix regelmäßig gewechselt werden. Da das Präfix vom Provider zugewiesen wird, ist der Provider dafür verantwortlich. Zweitens muss der Interface Identifier regelmäßig gewechselt werden. Da der Interface Identifier vom System zugewiesen wird, ist der Anwender bzw. dessen Administrator dafür verantwortlich.

Auf dem Weg dorthin wurden im Jahr 2007 für IPv6 die sogenannten Privacy Extensions eingeführt [RFC 4941]. Mit Privacy Extensions wird zusätzlich zur statischen Interface-ID in regelmäßigen Abständen eine jeweils neue pseudozufällige Interface-ID erzeugt; die daraus gebildete IP-Adresse wird auch als temporäre IP-Adresse bezeichnet. Damit sollten einige berechtigte Bedenken berücksichtigt werden. Es zeigt sich jedoch, dass der Einsatz von Privacy Extensions allein nicht ausreicht, um alle Bedenken auszuräumen.

Kürzlich wurden zudem sogenannte Opaque Interface-IDs eingeführt [RFC 7217]. Diese Interface-IDs sind mit Hilfe einer Einweg-Funktion gewählt, d. h. sie lassen keinen Rückschluss auf die MAC-Adresse oder andere Merkmale zu. Die Interface-IDs werden in Abhängigkeit vom Präfix und eines geheimen Schlüssels erzeugt. Bleibt der geheime Schlüssel konstant, dann bleibt auch die Interface-ID für ein festes Präfix konstant; wird der Schlüssel dagegen regelmäßig gewechselt, dann ergibt sich derselbe Effekt wie bei Privacy Extensions. Opaque Interface-IDs sollen EUI-64-Identifier ablösen und sind auch als Alternative zu Privacy Extensions gedacht.

## 2 Privatsphäre

Angriffe auf die Privatsphäre eines Anwenders können von einer oder mehreren End-Sites oder von einem Angreifer en-route erfolgen. Eine End-Site könnte beispielsweise eine Nachrichten-Site ein, auf der auch Werbung angezeigt wird. Angreifer en-route können beispielsweise Mitarbeiter von Netzbetreibern oder von Geheimdiensten sein. Die Angriffsziele bestehen jeweils darin, einzelne Nutzer zu verfolgen, zu profilieren oder zu identifizieren.

In diesem Abschnitt wird für drei unterschiedliche Szenarien die Tauglichkeit von NAT im Vergleich mit Privacy Extensions und Opaque Interface-IDs zur Wahrung der Privatsphäre diskutiert, vgl. auch [BVA 2013, Abschnitt 8.5]. Dazu ist zunächst zu definieren, was eigentlich Wahrung der Privatsphäre bedeutet.

- Das erste Ziel kann darin bestehen, als Client einer End-Site nicht ausfindig

gemacht werden zu können, d. h. ein Dienstanbieter (beispielsweise eine Nachrichtenseite) soll die Nutzungen des Dienstes zu verschiedenen Zeiten von einer bestimmten Site aus nicht miteinander korrelieren können. Mit anderen Worten, es soll nicht möglich sein, verschiedene Kommunikationsvorgänge einer Site zuzuordnen.
- Das zweite Ziel kann darin bestehen, als Client in einer Gruppe anderer Clients innerhalb einer Site nicht verfolgt werden zu können, d. h. ein Dienstanbieter mag zwar die Zugehörigkeit eines Nutzers zu einer Site nachverfolgen, aber nicht, welcher Client innerhalb der Site den betreffenden Dienst verwendet. Mit anderen Worten, es soll nicht möglich sein, zwischen den Clients einer Site zu differenzieren.
- Das dritte Ziel kann darin bestehen, als einzelner mobiler roaming Client nicht verfolgt werden zu können.

## 2.1 Szenario 1 – Heimnutzer

In diesem Szenario betrachten wir einen Nutzer, beispielsweise einen Heimnutzer, der von seinem ISP ein /56-Präfix zugewiesen bekommt.

Wird dem Nutzer über einen längeren Zeitraum dasselbe Präfix zugewiesen, dann kann die Site des Nutzers innerhalb dieses Zeitraums verfolgt werden. Die Verwendung von Privacy Extensions oder wechselnden Opaque Interface-IDs verschleiert zwar den einzelnen Client, aber nicht die Site. Selbst eine Verwendung von wechselnden Subnet-IDs bringt keinen Gewinn an Privatsphäre, da die Site nach wie vor am Präfix zu erkennen ist. Der Einsatz von NAT hilft an dieser Stelle ebenfalls nicht weiter.

Werden Präfix (vom ISP) und Subnet-ID (vom Nutzer) dynamisch vergeben, reicht das allein jedoch auch nicht aus. Wenn die Interface-IDs statisch vergeben werden, etwa über SLAAC oder pseudozufällig über DHCPv6, dann verraten die Interface-IDs die Clients innerhalb der Site und damit auch die Site an sich.

Um eine dauerhafte Korrelation von Zugriffen allein auf Basis der IP-Adresse zu verhindern, müssen sowohl das Präfix als auch die Interface-ID und möglichst auch die Subnet-ID dynamisch vergeben werden. Wird also das Präfix regelmäßig gewechselt, dann helfen sowohl Privacy Extensions als auch Opaque Interface-IDs.

## 2.2 Szenario 2 – Nutzer einer Site

In diesem Szenario betrachten wir eine Site mit statischem Präfix und einer signifikanten Anzahl von Nutzern, zwischen denen von außen eine Differenzierung nicht möglich sein soll.

In diesem Szenario helfen Privacy Extensions genauso wie NAT oder die Verwendung eines Proxys, das Aufspüren eines bestimmten Clients zu vermeiden. Opaque Interface-IDs helfen nur dann weiter, wenn auch der Schlüssel (siehe oben) regelmäßig gewechselt wird, da andernfalls die Interface-IDs innerhalb einer Site konstant bleiben.

Bei Verwendung der Privacy Extensions oder Opaque Interface-IDs bleibt das Ende-zu-Ende-Prinzip gewahrt. Im Fall von NAT würde das Ende-zu-Ende-Prinzip wieder aufgegeben. Bei Verwendung eines Proxys bliebe das Ende-zu-Ende-Prinzip erhalten und dennoch würden ausgehende Verbindungen von einer einzigen IP-Adresse kommend erscheinen. Da man auf dem Proxy auch gleich Content- und Malware-Filterung vornehmen kann, ist die Verwendung von Proxys gegenüber NAT oder Privacy Extensions im Unternehmensumfeld in der Regel die bessere Wahl.

## 2.3 Szenario 3 – Mobile roaming Clients

Dieses Szenario hat Ähnlichkeit zu Szenario 1 mit dynamischer Vergabe des Präfixes. Hierbei wird ein einzelner mobiler Client betrachtet, der sich von Netz zu Netz bewegt (Roaming), beispielsweise ein Smartphone.

Clients, deren Interfaces über SLAAC konfiguriert werden, bekommen bisher stets dieselbe Interface-ID, beispielsweise den EUI-64-Identifier. Ein roaming Client kann so über die Interface-ID über die Netzgrenzen hinweg verfolgt werden. Neben den bereits bestehenden Bedenken in Bezug auf die Wahrung der Privatsphäre kommt als potenzielle Bedrohung hinzu, dass hierüber ein Bewegungsprofil des Nutzers erstellt werden kann.

Die Privacy Extensions wurden dafür entworfen, um in genau diesem Szenario Abhilfe zu schaffen, indem regelmäßig eine zufällige temporäre Interface-ID gewählt wird. Opaque Interface-IDs helfen in diesem Szenario dagegen nur dann, wenn der Schlüssel (siehe oben) regelmäßig gewechselt wird.

An dieser Stelle würde auch NAT ggf. helfen, wenn alle Betreiber der besuchten Netze dies konsequent durchführen würden. Hierbei würde jedoch die Verantwortung zur Wahrung der Privatsphäre in die Hände der einzelnen Betreiber gelegt. Daher ist es vorzuziehen, die eigene Privatsphäre eigenverantwortlich durchzusetzen und Privacy Extensions zu nutzen oder bei Verwendung von Opaque Interface-IDs den Schlüssel regelmäßig zu wechseln.

## 3 Andere Möglichkeiten zur Identifizierung

Neben IP-Adressen gibt es viele Möglichkeiten zur zuverlässigen Identifizierung oder Verfolgung von Nutzern. Einige dieser Möglichkeiten zur Identifizierung oder zur Verfolgung lassen sich kaum vermeiden:
- Unterschiede in der Implementierung von Netzwerkprotokollen, beim SSL/TLS-Handshake, in der Reihenfolge und dem Inhalt von HTTP-Headern oder bei HTML-Stilelementen lassen ein Fingerprinting zu, mit dessen Hilfe ein Client mit hoher Wahrscheinlichkeit identifiziert oder verfolgt werden kann [Tillmann 2013].[2]
- Daneben kann ein Browser über JavaScript oder Flash von sich aus sehr viele Informationen preisgeben. Diese umfassen Systeminformationen, installierte Schriften, Zeitzone, Bildschirminformationen usw. Mit diesen Daten kann ein Client mit hoher Wahrscheinlichkeit identifiziert werden [Tillmann 2013].

Einem Beobachter en-route stehen sogar noch weitere Möglichkeiten zur Verfügung. Wenn der Benutzer bestimmte Dienste in Anspruch nimmt, die einzeln oder in Kombination individuell sind, dann kann der Client auch daran identifiziert werden. Beispiel hierfür ist die Nutzung einer individuellen Menge von Nachrichten-Seiten, oder die Nutzung individueller Dienste, etwa der Abruf von E-Mail von einem bestimmten Server.

Die Abwehr aller genannten Möglichkeiten ist nicht trivial und führt in der

Regel zu einer schlechteren Benutzbarkeit oder zu erheblichen funktionalen Einschränkungen.

## 4 Schlussfolgerungen

Die Privatsphäre wird durch IPv6 nicht mehr oder weniger bedroht, als durch IPv4. Die Nutzung von EUI-64 Interface-IDs ist aus Datenschutzsicht unglücklich, dies wurde aber durch die Einführung von Privacy Extensions und Opaque Interface-IDs behoben.

Mechanismen wie NAT oder Proxys können hier in einigen Szenarien zur Wahrung der Privatsphäre beitragen, ebenso die dynamische Vergabe von Präfixen. Jedoch sollte man dabei Folgendes bedenken: Die IP-Adresse ist nur eine Möglichkeit, Nutzer zu verfolgen.

Auf Anwendungsebene hinterlassen vor allem aber nicht nur Browser weitere Spuren, die zur Verfolgung von Nutzern geeignet sind. Auch ohne IP-Adressen gibt es bereits sehr umfangreiche Möglichkeiten, denen ein Anwender kaum entgehen kann. Die Frage, ob statische IP-Adressen eine Bedrohung der Privatsphäre darstellen, wird daher in der Regel überbewertet [Donn 2011]. Wer gezielt Anonymität im Netz sucht, sollte unabhängig vom genutzten Netzwerkprotokoll einen entsprechenden Dienst in Anspruch nehmen.

## 5 Verweise


[BVA 2013] C. Schmoll et al.: IPv6 – Migrationsleitfaden für die öffentliche Verwaltung. Bundesverwaltungsamt, 2013.

[Donn 2011] L. Donnerhacke: Kommentar: IPv6 und der Datenschutz. Heise Online, 2011, http://heise.de/-1375692.

[DSBL 2011] Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Datenschutz bei der Einführung des Internet-Prokolls Version 6 (IPv6). Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz, 2011.

[RFC 1918] Y. Rekhter et al.: Address Allocation for Private Internets. IETF Best Current Practice, Februar 1996.

[RFC 4941] T. Narten, R. Draves, S. Krishnan: Privacy Extensions for Stateless Address Autoconfiguration in IPv6. IETF Draft Standard, September 2007.

[RFC 7217] F. Gont: A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC). IETF Draft Standard, April 2014.

[Schaar 2011] P. Schaar (Hrsg.): Internetprotokoll Version 6 (IPv6) – Wo bleibt der Datenschutz?

[Tillmann 2013] H. Tillmann: Browser Fingerprinting: Tracking ohne Spuren zu hinterlassen. Diplomarbeit, Humboldt-Universität zu Berlin, 2013. http://bfp.henning-tillmann.de/downloads/Henning%20Tillmann%20-%20Browser%20Fingerprinting.pdf.


1 Die Großen RIRs ARIN, RIPE und APNIC haben ihren jeweils letzten /8-Block bereits angebrochen, siehe https://www.arin.net/announcements/2014/20140423.html, http://www.ripe.net/internet-coordination/news/announcements/ripe-ncc-begins-to-allocate-ipv4-address-space-from-the-last-8 bzw. http://www.apnic.net/publications/news/2011/final-8.

2 Siehe beispielsweise auch https://panopticlick.eff.org/

Thilo Weichert

# Weshalb Deutschland Edward Snowden um Einreise bitten muss

## Zusammenfassung

„Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur *verfassungsrechtlichen Identität der Bundesrepublik Deutschland*, für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss“.[1] Mit dieser Aussage des Bundesverfassungsgerichtes (BVerfG) ist die Richtung vorgegeben, wie angesichts der umfassenden Überwachung des Internetverkehrs auch von deutschen Nutzenden durch die Geheimdienste der USA und Großbritanniens, der National Security Agency (NSA) und des Government Communications Headquarters (GCHQ), die deutschen Stellen vorgehen müssen. Die folgenden Erwägungen kommen zu dem Ergebnis, dass die verantwortlichen Stellen in der Bundesrepublik, insbesondere die Bundesregierung, verpflichtet sind, den in Moskau vorläufig Asyl genießenden Edward Snowden zu bitten, nach Deutschland zu kommen und *Auskunft über seine Erkenntnisse zur Internetüberwachung* durch NSA und GCHQ zu geben.

## Rahmenbedingungen

Es wird im Folgenden davon ausgegangen, dass NSA und GCHQ eine anlasslose sehr umfassende Überwachung auch des in Deutschland generierten Internetverkehrs durchführen, wodurch nicht nur politische und wirtschaftliche Spionage betrieben wird, sondern auch eine Massenerfassung und -auswertung der Internetnutzung der gesamten Bevölkerung. Hiermit werden die im Grundgesetz (GG) und in der Europäischen Grundrechte-Charta (EuGRCh) garantierten Grundrechte verletzt. Dies sind insbesondere das in Art. 10 GG geschützte Telekommunikationsgeheimnis und die aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG geschützten Grundrechte auf informationelle Selbstbestimmung[2] und auf Gewährleistung der Integrität und

Vertraulichkeit der eigenen informationstechnischen Systeme[3]. Auf europäischer Ebene sind diese Grundrechte in Art. 7, 8 EuGRCh zugesichert. Zusammenfassend kann von der Notwendigkeit des Schutzes informationeller oder digitaler Grundrechte im Internet gesprochen werden.[4]

Zum digitalen Grundrechtsschutz gehört zum einen die *materiell-rechtliche Beachtung der Grundrechte*, also etwa des Rechts auf informationelle Selbstbestimmung. Der Schutz hat zugleich auch eine technisch-organisatorische sowie eine prozedurale Komponente. Von grundrechtlich zentraler Bedeutung ist die Beachtung des jeweiligen Zwecks einer Datenverarbeitung sowie die Beachtung der „informationellen Gewaltenteilung".[5] Und nur durch Kenntnis der Datenverarbeitung kann informationelle Selbstbestimmung wie auch Rechtsschutz realisiert werden.

Das BVerfG hat festgestellt, dass die vorsorgliche anlasslose Speicherung von personenbezogenen Daten im Internet zu schwerwiegenden Grundrechtseingriffen führt, weil diese Speicherung sich auf „Alltagshandeln bezieht, das im Miteinander elementar und für die Teilnahme am sozialen Leben der Welt nicht mehr verzichtbar ist". Die automatisierte Auswertung dringe bis in die Intimsphäre ein.[6] Diese Speicherung könne „ein diffus bedrohliches Gefühl des Beobachtetseins hervorrufen, das eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen kann".[7] Zwar gebe es kein absolutes „Verbot einer Speicherung von Daten auf Vorrat", doch unterliegt diese Speicherung *hohen rechtlichen, technischen und organisatorischen Anforderungen* unter strenger Beachtung der Verhältnismäßigkeit.[8] Diese Bewertung hat der Europäische Gerichtshof (EuGH) in seinem Urteil zur Vorratsdatenspeicherung vom 08.04.2014 umfassend für die gesamte Europäische Union und die in der EuGRCh garantierten Grundrechte bestätigt.[9] Die durch die NSA und das GCHQ durchgeführten Maßnahmen zur Überwachung des Internet entsprechen nicht ansatzweise den vom BVerfG und dem EuGH gestellten Anforderungen.

Derartige Grundrechtseingriffe über das Internet lassen sich nicht vollständig verhindern. Für eine weitgehende Reduzierung der Grundrechtsgefährdung ist ein *Zusammenwirken von verschiedenen Stellen und Personen* nötig. Hierzu gehören die betroffenen Nutzenden selbst sowie Telekommunikations- und Telemediendienste anbietende private Stellen, denen es auferlegt bleibt, insbesondere technische kommunikationsbezogene Schutzvorkehrungen, z. B. durch Verschlüsselung, vorzunehmen bzw. anzubieten. Für diese Vorkehrungen ist es erforderlich, eine möglichst genaue Kenntnis der Bedrohungen zu haben. Neben diesen nötigen und möglichen Maßnahmen des Systemschutzes und des Selbstschutzes besteht die Notwendigkeit von staatlichen Maßnahmen. Zum einen sind die Gesetzgeber gefordert, durch rechtliche Vorkehrungen die digitalen Kommunikationsvorgänge zu sichern und damit die Freiheiten im Internet zu gewährleisten. Derartige Regelungen liegen in der Verpflichtung zu technisch-organisatorischen Vorkehrungen sowie in der Gewährleistung von Kenntnis- und Rechtsschutzmöglichkeiten für die Grundrechtsträger (Art. 19 GG, Art. 47 EuGRCh). Inwieweit die deutschen und der europäische Gesetzgeber insofern das Notwendige geregelt haben, kann hier nicht weiter vertieft werden.

*Träger ausländischer Staatsgewalt* unterliegen deutschen und europäischen Gesetzen, soweit diese tangiert werden. Derartige Träger sind die NSA und das GCHQ. Ob sich Träger auswärtiger Staatsgewalt an die Grenzen des deutschen oder europäischen Rechts halten, ist für die Bürgerinnen und Bürger allerdings schwer überprüfbar. Die Eingriffe bei der Internetüberwachung erfolgen heimlich und sind für die Nutzenden regelmäßig nicht erkennbar. Rechtsschutz ist praktisch unmöglich.[10] Auch völkerrechtlich gestaltet sich eine Kontrolle schwierig, sofern die Eingriffe nicht im Inland erfolgen bzw. von geschütztem Gelände wie Botschaften oder Konsulaten ausgeübt werden.[11]

## Grundrechtliche Schutzpflichten

„Die Grundrechte binden in ihrem sachlichen Geltungsumfang die deutsche öffentliche Gewalt auch, soweit Wirkungen ihrer Betätigung außerhalb der Bundesrepublik Deutschland eintreten".[12] Deutsche Hoheitsträger sind verpflichtet, bei ihrem gesamten Handeln die verfassungsmäßigen Grundrechte zu schützen und zu verteidigen. Dies gilt angesichts der existenziellen *Bedeutung von Information und Kommunikation für unsere Informationsgesellschaft* insbesondere auch im Hinblick auf unsere Kommunikationsordnung. Die Abhängigkeit von persönlicher Entfaltung, der Freiheitswahrnehmung, des beruflichen und wirtschaftlichen Handelns, der Wissensgenerierung und -verarbeitung und der demokratischen Prozesse verpflichtet die staatliche Gewalt, die Funktionsfähigkeit der Kommunikationsinfrastruktur und den Schutz ihrer Nutzung zu gewährleisten.[13]

Diese Pflicht wird aus dem *objektiv-rechtlichen Schutzgehalt der Grundrechte* abgeleitet. Grundrechte entfalten ihre Wirkkraft als verfassungsrechtliche Wertentscheidungen durch die Gesetze. Den Hoheitsträgern obliegt es, im Rahmen dieser Gesetze eine optimale Umsetzung der Grundrechte zu sichern. Die Schutzpflicht gebietet es u. a., „dafür Sorge zu tragen, dass informationeller Selbstschutz für Einzelne tatsächlich möglich ist".[14]

„Die Schutzverpflichtung des Staates muss umso ernster genommen werden, je höher der *Rang des in Frage stehenden Rechtsgutes* innerhalb der Wertordnung des Grundgesetzes anzusetzen ist".[15] Bei widerstreitenden Verfassungswerten muss eine Abwägung mit dem Ziel eines möglichst schonenden Ausgleichs stattfinden. Die Menschenwürde aus Art. 1 Abs. 1 GG (Art. 1 EuGRCh) spielt dabei eine zentrale Rolle, wobei die „Verfassungswerte in ihrer Beziehung zur Menschenwürde als dem Mittelpunkt des Wertesystems der Verfassung zu sehen" sind.[16] Die Schutzpflichten bestehen für alle staatlichen Gewalten, also nicht nur die Legislative, sondern auch die Judikative und die Exekutive, und gelten nicht nur bei der Norminterpretation und -anwendung, sondern auch bei schlicht-hoheitlichem Handeln.[17]

Grundrechtlich begründete Schutzaufträge und -pflichten können auch in den *internationalen und globalen Raum* hineinwirken und sich gegen Eingriffe durch Träger anderer Staatsgewalten ak-

tivieren lassen. Die Nichtwahrnehmung der staatlichen Schutzaufgaben kann möglicherweise unter Berufung auf subjektive Rechte der Betroffenen gerichtlich geahndet werden. Die Verletzung kann aber auch durch das Parlament, etwa im Rahmen einer Organklage (Art. 93 Nr. 1 GG) oder einer abstrakten Normenkontrolle (Art. 93 Nr. 2 GG), in jedem Fall aber durch Entschließungen oder sonstige politische Maßnahmen sanktioniert werden.[18]

Staatliche Schutzaufträge können sich zudem *aus weiteren Verfassungsnormen* ergeben, etwa aus Art. 87f GG, wonach angemessene und ausreichende Kommunikationsdienstleistungen zu gewährleisten sind, oder aus Art. 91c GG, wonach Sicherheitsanforderungen an informationstechnische Systeme festgelegt werden müssen.[19]

Die staatlichen Einrichtungen verfügen bei der Umsetzung ihrer Schutzaufgaben grundsätzlich über einen *Gestaltungsspielraum*. Regelmäßig wird von der Verfassung die Zielsetzung vorgegeben, ohne dass sich hieraus bestimmte Handlungspflichten ergeben. Wohl unterliegen die Einrichtungen einer Optimierungspflicht. Die Maßnahmen müssen zur Erfüllung des Gewährleistungsauftrages effektiv beitragen. Zur Effektivitätssicherung kann es gehören, fortlaufend zu überprüfen, ob Schutzerfolge erreicht werden und die ergriffenen Maßnahmen zu korrigieren sind.[20]

Unter Umständen kann sich die Gestaltungsfreiheit in einer Weise verengen, dass die Schutzaufgabe nur durch *bestimmte Maßnahmen* erfüllt werden kann.[21] Angesichts der großen Bedeutung der Freiheit der Kommunikation und der Nutzung des Internet kommt eine Reduzierung des politischen Gestaltungsermessens dahingehend in Betracht, dass die zuständigen Staatsorgane verpflichtet sein können, im internationalen Bereich tätig zu werden.[22]

Das verfassungsrechtlich gebotene Schutzniveau wird dann unterschritten, wenn keine *effektive Informationsmöglichkeit* über die für informationelle Eingriffe relevante Fakten eingeräumt wird, insbesondere um Maßnahmen des informationellen Selbstschutzes eigenverantwortlich und selbständig wahrnehmen zu können.[23]

## Informationspflicht

Das deutsche und das europäische Recht kennt umfangreiche Regelungen, die den Informationszugang der Presse sowie auch von Bürgerinnen und Bürgern zu Verwaltungsinformationen vorsieht. Diese Regelungen des Presserechtes, der *Informationsfreiheitsgesetze* oder des Verbraucherinformationsrechtes enthalten aber bisher keine Regelungen, die eine explizite Informationsbeschaffungspflicht zum Schutz der digitalen Grundrechte und der Informations- und Kommunikations-Infrastruktur vorsehen.

Art. 10 Abs. 1 Europäische Menschenrechtskonvention (EMRK) sieht vor, dass das Recht auf Meinungsfreiheit auch die Freiheit einschließt, Informationen zu empfangen. Seit 2006 hat der Europäische Gerichtshof für Menschenrechte (EGMR) aus Art. 10 EMRK immer wieder abgeleitet, dass staatliche Stellen verpflichtet sein können, auch ohne ausdrückliche gesetzliche Regelung Informationen bereit zu stellen und aufzubereiten, insbesondere wenn diese von hoher Relevanz für die öffentliche Diskussion sind.[24] Dieser Informationsanspruch besteht selbst gegenüber Nachrichtendiensten.[25] Zwar gilt dieser Anspruch grundsätzlich nur, soweit eine öffentliche Stelle schon im Besitz der Information ist. Besteht aber eine grundrechtlich begründete Beschaffungspflicht bzgl. bestimmter Informationen, so kann sich aus Art. 10 EMRK, Art. 11 EuGRCh, Art. 5 GG zusätzlich auch eine *Bereitstellungspflicht* ergeben.

## Informationsbedarf

Voraussetzung für eine staatliche Informierungspflicht ist, dass ohne die Information eine *Gefährdung für eine grundrechtliche Position von einer dritten Seite* vorliegt.[26] Es muss schlüssig sein, dass die öffentliche Gewalt „Schutzvorkehrungen entweder überhaupt nicht getroffen hat oder die getroffenen Regelungen und Maßnahmen gänzlich ungeeignet oder völlig unzulänglich sind, das gebotene Schutzziel zu erreichen".[27]

Die *Verletzung informationeller Grundrechte* durch die NSA und den GCHQ hat schon in der Vergangenheit stattgefunden, findet offensichtlich weiterhin statt und droht auch für die Zukunft. Informationen über die Art des Vorgehens dieser Geheimdienste in der Vergangenheit sind geeignet, angemessene Abwehrmaßnahmen angesichts der fortgesetzt bestehenden Gefahr zu ergreifen, da davon auszugehen ist, dass die informationellen Angriffe nicht beendet, sondern auf der Basis der modernsten technischen Mittel weiterentwickelt werden.

## Informationsverweigerung

Es wäre naheliegend, dass sich die öffentlichen Stellen in Deutschland die hinsichtlich der Grundrechtsgefährdung nötigen Informationen von den *verantwortlichen britischen und US-amerikanischen Stellen* besorgen. Dies wurde auch tatsächlich seit Bekanntwerden der Überwachungsmaßnahmen im Sommer 2013 immer wieder versucht. Die verantwortlichen Stellen in Großbritannien und in den USA haben aber jegliche substanziierte überprüfbare Auskunft verweigert.

Dies wird z. B. durch *Bundesinnenminister* Thomas de Maizière hinsichtlich der Überwachung durch US-Dienste bestätigt: „Die Informationen sind bis heute unzureichend. … Was die USA an Aufklärungsmaßnahmen tun, ist zwar ganz überwiegend ihrem Sicherheitsbedürfnis geschuldet, aber sie tun es in einer übertriebenen, maßlosen Anwendung. … Wenn zwei Drittel dessen, was Edward Snowden vorträgt oder was unter Berufung auf ihn als Quelle vorgetragen wird, stimmen, dann komme ich zu dem Schluss: Die USA handeln ohne Maß. … Meine Erwartungen an einen Erfolg weiterer Gespräche (mit den USA, T.W.) sind niedrig." In Hinblick auf das durch den britischen GCHQ propagierte „Mastering the Internet" ergänzte de Maizière: „Ja, das bereitet uns allen Sorgen. Das Internet, auch in seinen Stärken, lebt von der Freiheit. Doch jetzt ist durch die explosionsartige Vermehrung der Kommunikation ein Ordnungs- und Auswahlproblem entstanden – verschärft durch die Marktmacht von Unternehmen. Wenn ein großer Netz-Provider und ein Content-Betreiber sich zusammentun, dann können sie das In-

ternet steuern und Inhalte setzen. Da muss ich nicht über staatliche Zensur reden".[28]

Was das deutsche für die Spionageabwehr zuständige *Bundesamt für Verfassungsschutz* (BfV) über die Spionage durch die NSA weiß, erläuterte deren Präsident Hans-Georg Maaßen in einem Interview: „Auch wenn es Sie überrascht – wir wissen es nicht genau. Die Dokumente des NSA-Enthüllers Snowden sind voller Hinweise, aber ohne Beweise. Wir gehen nach wie vor davon aus, dass sich die Amerikaner in Deutschland an deutsches Recht halten. … Wir haben weder valide Erkenntnisse, dass die Amerikaner Breitbandkabel in Deutschland anzapfen, noch ob aus der US-Botschaft in Berlin das Handy der Kanzlerin abgehört worden ist. … (Ich habe) den Eindruck, dass die Amerikaner nach wie vor nationale Interessen als die zentrale Richtlinie ihrer Politik ansehen. Sie tun das sehr selbstbewusst. … Die Deutschen waren in der Vergangenheit vielleicht zu gutgläubig und leichtfertig im Umgang mit ihren Daten".[29]

## Informationsangebot

Edward Snowden hat über seinen Anwalt signalisiert, dass er Informationen gegenüber Stellen in Deutschland, etwa dem NSA-Untersuchungsausschuss, zu geben bereit ist: „Ich bin gerne bereit, vor dem Untersuchungsausschuss auszusagen und knüpfe dies grundsätzlich an *keine Bedingungen*". Wie detailreich sich Snowden äußern „kann und will", hinge letztlich von den Umständen ab, unter denen die Aussage erfolgt. Dessen Aufenthaltsgenehmigung bzw. vorläufiges Asyl in Russland läuft Ende Juli 2014 ab. Der Aufenthalt in Russland ist an die Bedingung geknüpft, dass Snowden den USA nicht (weiter) schadet. Die USA suchen Snowden mit internationalem Haftbefehl.[30] Bisher war eine umfassende ernst zu nehmende Zeugenbefragung weder durch das Europaparlament noch durch den Europarat möglich.

Die von Snowden *zu erwartenden Informationen* gehen über das hinaus, was bisher von ihm und über ihn bekannt wurde. Ex-Anwalt, Blogger und Kolumnist Glenn Greenwald, der Zugang zu den Snowden-Unterlagen hat, erklärte: „Die Dokumente, die bislang veröffentlicht wurden, sind nur ein kleiner Teil des gesamten Materials, das uns Edward Snowden übergeben hat. Es gibt zahlreiche Dokumente mit brisanten Informationen darüber, was die NSA getan hat und was sie weiterhin tut, die noch gar nicht veröffentlicht wurden." Um sich zu schützen, sei Snowden derzeit nicht mehr im Besitz der Dokumente. Diese Notwendigkeit des Selbstschutzes würde in Deutschland nicht mehr bestehen. Zudem erläutert Greenwald: „Er weiß viele Dinge über die NSA, die nicht in den Dokumenten stehen. Er kann erklären, wie das ganze System funktioniert. Dem Untersuchungsausschuss kann er die bereits veröffentlichten Informationen erklären und neue Informationen geben".[31] Nach Presseberichten hat Snowden die erlangten Dateien „in Kategorien sortiert, die die verschiedenen Geheimprogramme der NSA dokumentieren, etwa Überwachung anderer Staaten oder die Internet-Infrastruktur. Allein die Dokumente des britischen Geheimdienstes GCHQ, die er gesondert abgespeichert hat, umfassen rund 50.000 Dateien. In den Papieren finden sich diverse Anhaltspunkte, die auch für die Untersuchung in Deutschland wichtig sind".[32]

Snowden hatte, so sein Anwalt, eine „innerhalb der US-Geheimdienststruktur einzigartige berufliche Stelle" inne; Er war „persönlich mit der Durchführung und Leitung von Massenüberwachungsmaßnahmen" befasst.[33] Er hatte also *Einblick in die grundrechtsrelevante operative Arbeit der NSA* und erhielt dadurch auch tiefe Einblicke in die Arbeit des GCHQ und anderer Geheimdienste. Snowden selbst erklärte gegenüber dem Europaparlament, er habe operativ gearbeitet und kenne deshalb das Innenleben der NSA ziemlich gut. Die NSA habe ihm die „Autorität verliehen, Kommunikation in aller Welt abzuhören. Ohne meinen Platz zu verlassen, hätte ich alle Mitglieder Ihres Komitees abhören können, genauso wie jeden normalen Bürger".[34]

*Alternative Informationsmöglichkeiten* zu einer umfassenden Befragung von Edward Snowden, die den deutschen rechtlichen Anforderungen entsprechen, sind nicht erkennbar.

## Gefährdung von Snowden

Vizekanzler Sigmar Gabriel riet Snowden von einem Asylgesuch in Deutschland ab: „Deutschland ist ein kleines Land, in dem der amerikanische Geheimdienst sehr genau weiß, wer hier was tut. Ich bin sicher, dass der Geheimdienst der USA versuchen würde, ihn unter Kontrolle zu bringen".[35] Snowden hat seine Informationserteilung nicht von einem bestimmten Schutzstatus abhängig gemacht. Er hat die Befugnis, über seine Selbstgefährdung zu befinden. Dessen ungeachtet würde die Informationsbereitschaft von Snowden gefördert, wenn er in Deutschland einen *sicheren Aufenthalt* zugesichert bekäme. Möglich ist ein Asylantrag. Seit Sommer 2013 liegt ein Festnahmeersuchen der USA an Deutschland vor. Gemäß dem Rechtshilfeabkommen mit den USA ist eine Auslieferung ausgeschlossen, wenn Deutschland die Straftat, wegen der die Auslieferung gefordert wird, als Straftat mit politischem Charakter betrachtet. Die rechtliche Beurteilung obliegt zunächst dem Oberlandesgericht; bei einem Aufenthalt Snowdens in Berlin wäre dies das Kammergericht. Wenn es die Auslieferung ablehnt, wäre diese unzulässig. Wenn es die Auslieferung für zulässig hält, kann der Bundesjustizminister diese immer noch ablehnen. Er könnte auch schon vorab erklären, dass er auf jeden Fall eine Auslieferung Snowdens ablehnt.

## Erwägungen gegen eine Information durch Snowden

Eine Befürchtung besteht, dass bei einer deutschen Befragung von Snowden die US-Dienste den Informationsaustausch mit Deutschland einschränken würden. Bundesinnenminister Thomas de Maizière erklärte, ohne die Amerikaner sei man „taub und blind". Informell habe die US-Regierung die Bundesregierung wissen lassen, ein dauerhafter Aufenthalt von Snowden werde als Affront empfunden.[36] Diese Erwägungen basieren jedoch bisher auf Spekulationen. Angesichts der wichtigen Bedeutung Deutschlands in Europa und als politischer Partner für die USA müssen solche Ankündigungen und Statements als diplomatische Abwehrversuche verstanden werden. Es steht einem souve-

ränen demokratischen Staat nicht an, auf mögliche grundrechtsrelevante Informationen lediglich aus der Befürchtung heraus zu verzichten, dadurch könnten nicht näher substantiierte Informationen von den USA vorenthalten werden.

Ein Argument gegen eine Informationsbeschaffung bei Snowden ist, dass dies die *politischen Beziehungen* zu den USA beeinträchtigen würde und damit dem Staatswohl abträglich wäre. Auch diese Annahme ist Spekulation. Richtig ist, dass US-Vertreter entsprechende Ankündigungen gemacht haben. Richtig ist aber auch, dass die USA gegen ein grundrechtlich begründetes Vorgehen der Bundesrepublik wirksam keine politischen oder diplomatischen Sanktionen durchführen könnten. Die USA sind selbst bei ihrem Vorgehen im eigenen Interesse wenig rücksichtsvoll gegenüber anderen Staaten, wie sich z. B. bei der Internetüberwachung zeigt, und können keine Rücksichtnahme auf ihre Befindlichkeiten erwarten.

Letztlich kann und muss den USA vermittelt werden, dass eine umfassende Aufklärung der NSA im Interesse eines digitalen Grundrechtsschutzes *in deren eigenen Interesse* liegt. Dies gilt in Bezug auf das weltweite Ansehen des Landes. In einer einstimmig verabschiedeten Resolution hat die Generalversammlung der Vereinten Nationen am 22.11.2013 herausgestellt, dass die im Raum stehende Massenüberwachung des Internet eine Verletzung der Gewährleistung der allgemeinen Erklärung der Menschenrechte und des Paktes für politische und zivile Rechte darstellt.[37]

Es kann davon ausgegangen werden, dass die Vorgehensweisen von NSA und GCHQ gegen geltendes *einfaches und Verfassungsrecht* in den USA und in Großbritannien verstoßen. Entsprechende Argumente wurden vielfach vorgetragen; vereinzelt wird dies durch Gerichtsentscheidungen bestätigt.[38]

Ein von *deutscher Nachrichtendienst-Seite* bestehender Einwand gegen eine umfassende Information direkt bei Edward Snowden besteht darin, dass schädliche Geheimnisse über die deutschen Dienste aufgedeckt werden könnten, etwa über die Kooperationen mit der NSA und dem GCHQ.[39] Diese Befürchtung spricht eher für eine Einladung Snowdens als gegen diese: Durch eine offizielle direkte Befragung Snowdens könnten die deutschen Einrichtungen die nötigen Informationen selbst erheben, anstelle sie irgendwann über Journalisten vermittelt in der Presse zu lesen. Geheimhaltungsbedürftige Informationen könnten gezielt vertraulich behandelt werden.

Anders als manch informationstechnisch hoch gerüstete autoritäre Staaten fühlen sich die USA ebenso wie Europa und Deutschland von dem aus dem Neuen Testament stammenden Satz verpflichtet: „Die *Wahrheit* wird euch frei machen."[40] Dieser aufklärerische Ansatz ist eine Grunderwägung jeder freiheitlich-demokratischen Gesellschaft. Sollte Snowden die Unwahrheit mitteilen, so sind Vertreter der betroffenen Geheimdienste und Staaten eingeladen, dies richtig zu stellen. Bisher basieren die wenigen erkannten Fehler in den Snowden-Enthüllungen nicht auf falschen Grundinformationen, sondern auf Fehlinterpretationen der Dokumente.[41]

## Abschließende Erwägungen

Edward Snowden tat mit der NSA das, was die NSA mit der Welt tut – er spionierte sie aus. Die Motivation der NSA bei ihrer Spionagetätigkeit ist nur begrenzt ehrenhaft. Die Motivation Snowdens kann dagegen nur mit viel bösem Willen als unethisch verworfen werden. Letztlich geht es Snowden darum, digitale Grundrechte zur Geltung zu bringen gegen Bestrebungen eines digitalen US-Imperialismus. Snowdens Engagement zielt darauf ab, in unserer globalen Informationsgesellschaft die sich abzeichnende Kanibalisierung zu bremsen, bei der nicht das Recht, sondern die Macht des Stärkeren gilt. Journalisten, die als Informationsmittler zwischen Snowden und der Öffentlichkeit agieren, berichten, dass Snowden immer wieder ausdrücklich klargestellt hat, dass mit den von ihm ermöglichten Offenlegungen legitimen Operationen des Geheimdienstes nicht geschadet werden soll, sondern dass seine Medienpartner sich darauf beschränken sollen, die Auswüchse des informationstechnisch agierenden Sicherheitsstaates aufzudecken.[42]

Es ist ein Armutszeugnis für die demokratischen freiheitlichen Staaten auf der ganzen Welt, dass Snowden bisher nur in einem Staat wirksamen Schutz vor politischer Verfolgung finden konnte, der sich immer wieder durch das Ignorieren von Freiheit, Demokratie und Menschenrechten profiliert. Für einen der mächtigsten Staaten in der Europäischen Union mit einer wichtigen Stimme im globalen politischen Geschehen wie der Bundesrepublik sollte es – jenseits aller verfassungsrechtlichen Verpflichtungen – keine Überforderung darstellen, Snowden nicht nur um Einreise und Aufklärung zu bitten, sondern alles zu tun, um ihn vor Schaden zu schützen. Es ist nicht vermittelbar, weshalb wir von seinen Informationen profitieren, um weiterhin in Freiheit leben zu können und ihn weiterhin in ein Leben in sehr eingeschränkter Freiheit und unter der Aufsicht eines autoritären Staates zu zwingen.

1 BVerfG NJW 2010, 839 f. – Vorratsdatenspeicherung.

2 BVerfGE 65, 1 ff. = NJW 1984, 419 ff. – Volkszählung.

3 BVerfGE 120, 274, 313 ff. = NJW 2008, 822 ff. – Online-Durchsuchung.

4 Dazu Weichert, Codex Digitalis Universalis, in Schmidt/Weichert, Datenschutz, 2012, S. 345 ff.

5 BVerfG NJW 1984, 419, 428.

6 BVerfG NJW 2010, 838.

7 BVerfG NJW 2010, 839.

8 BVerfG NJW 2010, 833.

9 EuGH U. v. 08.04.2014, Az. C-293/12, C-594/12 – Vorratsdatenspeicherung.

10 Hoffmann-Riem, Freiheitsschutz in den globalen Kommunikationsinfrastrukturen, JZ 2014, 55.

11 Ewer/Thienel, Völker-, unions- und verfassungsrechtliche Aspekte des NSA-Datenskandals NJW 2014, 30 ff.; Wolf, Der rechtliche Nebel der deutsch-amerikanischen „NSA-Abhöraffäre" JZ 2013, 1039 ff.

12 BVerfGE 57, 9, 23.

13 BVerfG NJW 2010, 838 – Vorratsdatenspeicherung.

14 BVerfG NJW 2013, 3087 – Schweigepflichtentbindung II.

15 BVerfGE 39, 1, 42.

16 BVerfGE 39, 1, 43.

17 Rupp, Die grundrechtliche Schutzpflicht des Staates für das Recht auf informationelle Selbstbestimmung im Pressesektor, 2013, S. 35.

18 Hoffmann-Riem (Fn. 10) JZ 2014, 57, 60.

19 Im Detail Hoffmann-Riem (Fn. 10) JZ 2014, 58 f.

20 Hoffmann-Riem (Fn. 10) JZ 2014, 62.

21 BVerfGE 77, 170, 215.

22 Ähnlich der Wissenschaftliche Dienst des Bundestags in einem Gutachten zur Ladung von Snowden vor dem parlamentarischen Untersuchungsausschuss: „Reduzierung des Ermessens auf Null", Blome/Gude/Pfister/Schindler/Stark, Die Zeugen-Verweigerer, Der Spiegel 16/2014, 21.

23 BVerfG NJW 2013, 3087 f.

24 Zuletzt EGMR U. v. 28.11.2013, Österreichische Vereinigung v. Austria; zur deutschen Verfassungslage nach Art. 5 GG Wegener, Der geheime Staat, 2006, 475 ff.

25 EGMR U. v. 26.06.2913, Youth Initiative for Human Rights v. Serbia, DANA 2013, 164 f.

26 BVerfG NVwZ 2010, 704.

27 BVerfGE 77, 170, 215; 92, 26, 46.

28 „Die USA handeln ohne Maß", Der Spiegel 15/2014, 33.

29 Jakobs/Sigmund, Einspruch Herr Snowden! Handelsblatt 29.01.2014, 5.

30 Mitgeteilt über RA Wolfgang Kaleck, zit. nach: Goetz/Obermaier, „Snowden stellt keine Bedingungen für seine Aussage", SZ 12./13.04.2014, 1.

31 Obermaier, „Es ist noch längst nicht alles berichtet", SZ 11.04.2014, 31.

32 Blome/Gude/Pfister/Schindler/Stark (Fn. 22), Der Spiegel 16/2014, 22 f.

33 Kaleck (Fn. 30).

34 Blome/Gude/Pfister/Schindler/Stark (Fn. 22), Der Spiegel 16/2014, 22 f.

35 Zit. nach Petersen, Ein komplizierter Fall, Kieler Nachrichten 16.04.2014, 2.

36 Goetz/Mascolo/Leyendecker, Der unheimliche Zeuge, SZ 11.04.2014, 5.

37 United Nations General Assembly, The Right to Privacy in the digital Age, A/C.3/68/L45/45/Rev.1; DANA 1/2014, 30 f.

38 Z. B. District Court of Columbia, Klayman et al. V. Obama et al., Dec 16 2013; vgl. schon Westin, Privacy and Freedom, 1967, S. 330 ff.

39 Braun, Wachhunde mit Maulkorb, SZ 03.04.2014, 5.

40 Die Bibel, Johannes-Evangelium, Kap. 8 Vers. 32.

41 Greenwald in Obermaier (Fn. 31), SZ 11.04.2014, 31.

42 Luke Harding, Liebe NSA: Wie finden Sie mein Buch? SZ 19.-21.04.2014, 11.

### Pressemitteilung vom 06.06.2014 der Deutschen Vereinigung für Datenschutz e.V.

# Diese Geheimdienste sind nicht reformierbar

Die Deutsche Vereinigung für Datenschutz e.V. (DVD) erklärt ihre Unterstützung für die Aktion „Verfassung schützen – Geheimdienste abschaffen" der Humanistischen Union (http://www.verfasssung-schuetzen.de)

Die DVD hält eine Abschaffung dieser Dienste in der heutigen Form für das einzig rechtsstaatlich gebotene Mittel, um einen Neuanfang zur demokratischen Gestaltung bestimmter Ermittlungsbefugnisse zu schaffen, nachdem

- dem deutschen Auslandsgeheimdienst BND keine bessere Reaktion einfällt, als die amerikanischen Praktiken nachzuahmen und in Zukunft Daten in sozialen Medien per Schleppnetzfahndung auswerten zu wollen,
- der BND für eine umfassende Ausländerüberwachung auch im Inland verantwortlich zeichnet,
- der BND in großem Umfang Daten an den US-Geheimdienst NSA weitergibt,
- sich der BND über die NSA verfassungswidrig Daten auch über deutsche Staatsbürger beschafft
- Verfassungsschutzämter mit rechtsextremistischen Organisationen verstrickt sind,
- die „Kommunikationsdefizite" von Verfassungsschutzämtern bei den Ermittlungen gegen den „Nationalsozialistischen Untergrund (NSU) offenbar wurden,
- seit Bestehen der Dienste diese immer wieder in Skandale verwickelt waren,
- die deutsche Regierung aus Angst, ihre Dienste würden nicht mehr mit Geheiminformationen versorgt, die Menschenrechte der gesamten Bevölkerung zur Disposition stellt.

Die deutschen Geheimdienste sind für die Grundrechte der Menschen und für die öffentlichen Haushalte eine übergroße Belastung. Und sie richten mehr Schaden an als sie unserer demokratischen Gesellschaft nützen. Die über 60-jährige Geschichte der deutschen Dienste zeigt, dass sie in ihren bestehenden Strukturen nicht reformier- und kontrollierbar sind. Die Kontrolle durch Gerichte und das Parlament wird durch Geheimhaltungsregeln faktisch unmöglich gemacht.
Die DVD fordert, eine Generaldebatte über Aufgaben, Mittel, Kontrolle und rechtliche Grundlagen der Dienste zu führen. Voraussetzung hierfür ist das Abwickeln der bestehenden Organisationen und ein Neuanfang, bei dem folgende Aspekte berücksichtigt werden müssen:

- Die verfassungsrechtlich angelegte Trennung zwischen polizeilicher exekutiver und geheimdienstlicher Tätigkeit muss durch klare gesetzliche Vorgaben insbesondere im informationellen Bereich umgesetzt werden.
- Geheimdienstliche Vorfeldermittlungen dürfen nicht Großteile der Bevölkerung erfassen und müssen sich auf konkret definierte Bestrebungen und Verdachte beschränken.
- Zur umfassenden Kontrolle der neu zu schaffenden Organisation des Bundes

ist die Stelle eines Beauftragten mit einem eigenen professionellen Apparat einzurichten, der umfassende anlasslose Kontrollbefugnisse erhält und in Kooperation mit den Datenschutzkontrollbehörden Beschwerden überprüft und gegenüber dem Parlament berichtet.

- Kooperationen mit ausländischen Geheimdiensten sind parlamentarischen Berichts-, Kontroll- und Genehmigungsverfahren zu unterwerfen.

Wir rufen außerdem auf, den Aufruf zur Abschaffung des Inlandsgeheimdienstes auch als Einzelperson hier zu unterschreiben: http://www.verfassungschuetzen.de/aufruf/

Weitere Auskünfte erteilt Karin Schuler, Vorsitzende der DVD e.V. unter 0228/24 20 733

# Kirchensteuersperrvermerk

Schon in der DANA 1/2014 haben wir auf dieses Thema hingewiesen.
Aufgrund der immer noch bestehenden Aktualität erlauben wir uns einen erneuten (leicht erweiterten) Hinweis zum Thema Kirchensteuersperrvermerk.

Der Kirchensteuerabzug für Kapitalerträge soll im Regelfall ab 2015 automatisiert über die Kreditinstitute erfolgen. Dazu werden diese durch ein elektronisches Abrufverfahren die Religionszugehörigkeit ihrer Sparer beim Bundeszentralamt für Steuern (BZSt) erfahren.
Wer nicht wünscht, dass Banken, Versicherungen und Fondsgesellschaften die Religionszugehörigkeit automatisch mitgeteilt bekommen, kann dies durch einen Sperrvermerk beim BZSt (spätester Eingang beim BZSt bis zum 30.06.2014) verhindern. Die eventuelle anfallende Kirchensteuer wird dann wie bisher im Rahmen der Einkommenssteuererklärung abgeführt.
Bitte beachten Sie, dass sich in Zweifelsfällen aufgrund des Sperrvermerks das Finanzamt bei Ihnen melden und Sie zur Abgabe einer separaten Kirchensteuererklärung auffordern kann, falls Sie bisher keine Einkommenssteuererklärung abgegeben haben.

**Hinweise zur Beachtung:**
Das Formular, welches mit der Post geschickt werden muss, finden Sie hier: http://www.formulare-bfinv.de/ffw/action/invoke.do?id=010156
Sie können sich bei der Hotline des BZSt informieren: 0228/406-1240.
Bitte lesen Sie zu dieser Thematik auch den nebenstehenden Leserbrief von André Pospischil.

*Sehr geehrte Damen und Herren,*

*in der letzten Ausgabe der Datenschutz Nachrichten (DANA 1/14) fand ich auf Seite 16 einen Hinweis auf das Verfahren KiStA des Bundeszentralamts für Steuern. Mit diesem machten Sie auf die Möglichkeit zur Eintragung eines Sperrvermerks aufmerksam. Dies halte ich für einen wichtigen Beitrag um die Öffentlichkeit für dieses - auch aus meiner Sicht - wichtige Thema zu sensibilisieren. Vielleicht kann ich diese Ihre Ausführungen mit dem Folgenden um einen weiteren Aspekt ergänzen:*

*Da ich – auch als überzeugter Katholik – die zentrale Speicherung des Merkmals der Zugehörigkeit zu einer steuererhebenden Religionsgemeinschaft (§ 39e Abs. 2 Staz 1 Nr. 1 Einkommensteuergesetz) bereits im Hinblick auf das erhebliche Missbrauchspotential (vgl. Götz Aly / Karl Heinz Roth: /Die restlose Erfassung/, S. Fischer Verlag, Frankfurt 2005; Christiane Kuller: /Bürokratie und Verbrechen/, Oldenbourg Verlag, München 2013) mit gemischten Gefühlen sehe, hatte ich mich in den vergangenen mit der datenschutzrechtlichen Dimension der Thematik beschäftigt und die Ergebnisse in einer kleinen Ausarbeitung zusammengefasst (André Pospischil: /Kirchensteuer im 21. Jahrhundert,/ epubli, Berlin 2013, ISBN 978-3-8442-6927-7 <http://de.wikipedia.org/wiki/Spezial:ISBN-Suche/9783844269277>).*

*Im Ergebnis habe ich dabei festgehalten, dass die vorgenannte Datenspeicherung und -verwendung (§ 39e Abs. 2 Statz 1 Nr. 1 Einkommensteuergesetz) nach meiner Auffassung gegen § 4 BDSG verstößt, da nach dieser Vorschrift eine Speicherung personenbezogener Daten nur dann zulässig ist, wenn sie auf einer Rechtsgrundlage beruht, die in verfassungskonformer Weise in das Recht auf informelle Selbstbestimmung eingreift (vgl. Nomos Kommentar Simits zum BDSG, 7. Auflage, Rz. 14 zu § 4 BDSG). Die Rechtsgrundlage für die Speicherung des Merkmals der Zugehörigkeit zu einer steuererhebenden Religionsgemeinschaft (§ 39 e Abs. 2 Satz 1 Nr. 1 EStG) wird einzig für die Einbehaltung der Kirchensteuer auf Lohnsteuer und Abgeltungssteuer (ELStAM und KiStA) benötigt. Mit ihr wird damit ein Teil des Kirchensteuerverfahrens gesetzlich kodifiziert. Nach Art. 140 Grundgesetz i. V. m. Art. 137 Abs. 6 der deutschen Verfassung vom 11. August 1919 obliegt die Gesetzgebungskompetenz hierfür allein den Ländern. Im Einkommensteuergesetz als Bundesgesetz ist die fragliche Vorschrift somit deplatziert. Sie wurde von einem unzuständigen Gesetzgeber erlassen. § 39e Abs. 2 Satz 1 Nr. 1 EStG bietet damit aus meiner Sicht keine ausreichende Grundlage für die Speicherung der Religionszugehörigkeit.*

*Für Fragen oder weiterführende Hinweise zur angesprochenen Thematik stehe ich Ihnen – bei Bedarf – gern zur Verfügung.*

*Mit freundlichen Grüßen*

# TrueCrypt – Eine Erfolgsgeschichte ohne Happy End?

Am 29.05.2014 ging eine Eilmeldung durch das Internet: TrueCrypt ist unsicher.

TrueCrypt ist eines der beliebten kostenlos verfügbaren Verschlüsselungswerkzeuge. Die Programmierer erklären, dass TrueCrypt unsicher ist und dass man zu Bitlocker von Microsoft wechseln soll. Die bestehende Ratlosigkeit machte ersten Erklärungsversuchen Platz.[1]

TrueCrypt wird gerade von unabhängiger Stelle einem CodeReview unterzogen. Sicherlich gibt es die eine oder andere Stelle, wo die Programmierer hätten eleganter oder sauberer arbeiten können. Schwerwiegende Fehler bzw. Sicherheitsprobleme wurden dabei aber bisher nicht gefunden. Und deswegen wird an vielen Stellen auch weiterhin empfohlen, die vorherige Version 7.1a weiter zu nutzen (die aktuelle Version 7.2 ist funktional stark eingeschränkt und nur noch in der Lage, TrueCrypt Container zu entschlüsseln).

Auch der Autor dieses Artikels nutzt es weiter. Warum? Weil TrueCrypt als einzige dem Autor bekannte Verschlüsselungssoftware auf allen drei wesentlichen Betriebssystemen (Windows, Linux, MacOS) funktioniert.[2]

Was sind mögliche Gründe für das Ende von TrueCrypt? Von sogenannten National Security Lettern bis hin zu Demotivation des Projektteams wird alles diskutiert.

Die Zukunft von TrueCrypt steht in den Sternen. Eines scheint sicher, ein Nachfolgeprodukt wird wohl einen anderen Namen tragen. Es wird (genügend motivierte Entwickler vorausgesetzt) wahrscheinlich auf einen Fork (eine Weiterentwicklung durch ein neues Team, aufsetzend auf einem definierten Projektstand) hinauslaufen. Hier könnte sicherlich auch die Bundesregierung, vertreten durch das BSI, maßgeblich für mehr Datenschutz und Datensicherheit sorgen, in dem sie solch ein Projekt finanziell unterstützt.

Wem das Weiternutzen von TrueCrypt ab jetzt zu unsicher ist, findet an vielen Stellen im Internet Alternativen.

1 http://www.heise.de/security/artikel/Truecrypt-ist-unsicher-und-jetzt-2211475.html

2 http://www.heise.de/download/truecrypt.html




# BigBrotherAwards 2014

Die nachfolgenden kurzen Zusammenfassungen der Laudationes wurden von digitalcourage e.V. erstellt.
Weitere Details: https://www.bigbrotherawards.de/2014

## Politik: Das Bundeskanzleramt

Der BigBrotherAward 2014 in der Kategorie Politik geht an das Bundeskanzleramt für geheimdienstliche Verstrickungen in den NSA-Überwachungsskandal sowie unterlassene Abwehr- und Schutzmaßnahmen. Dem Bundeskanzleramt obliegen die oberste Fachaufsicht über den Auslandsgeheimdienst BND sowie die Kooperation der drei Bundesgeheimdienste untereinander und mit anderen Dienststellen im In- und Ausland. Die bundesdeutschen Geheimdienste arbeiten eng mit dem völker- und menschenrechtswidrig agierenden US-Geheimdienst NSA und anderen Diensten zusammen. BND und Bundesamt für Verfassungsschutz sind an Überwachungsinstrumenten, Spähprogrammen und Infrastrukturen der NSA beteiligt. Alte wie neue Bundesregierung haben mit Massenausforschung und Digitalspionage verbundene Straftaten und Bürgerrechtsverstöße nicht abgewehrt: Sie haben es sträflich unterlassen, die Bundesbürger und von Wirtschaftsspionage betroffene Betriebe vor weiteren feindlichen Attacken zu schützen.

## Verkehr: MeinFernbus GmbH in Berlin

Der BigBrotherAward 2014 in der Kategorie Verkehr geht an die „MeinFernbus GmbH“ für die Verpflichtung, zusammen mit einem Online-Ticket immer auch einen amtlichen Ausweis vorzeigen zu müssen. Dadurch wird das anonyme Reisen per Bus unmöglich. Eine gesetzliche oder sachliche Notwendigkeit für diese Ausweispflicht nennt die „MeinFernbus GmbH“ nicht. Man kann auch versuchen, beim Einsteigen bar zu bezahlen, geht dann aber das Risiko ein, dass der Bus evtl. ausgebucht ist und man nicht mehr mitfahren kann. Außerdem sind die bar bezahlten Tickets teurer als bei der Frühbuchung im Internet.

## Technik: Die „Spione im Auto“

Der Big Brother Award in der Kategorie Technik geht an die „Spione im Auto“, die uns bei jedem gefahrenen Meter über die Schulter schauen und dabei Datensammlungen anlegen – oder diese sogar in die „Cloud“ übertragen. Einen Schuldigen dafür zu benennen ist schwierig: Die Autohersteller verweisen einerseits auf gesetzliche Vorgaben, andererseits auf Drittanbieter, die z.B. Ortungs- oder Navigationsdienstleistungen im Auftrag des Fahrers erbringen. Dieser BigBrotherAward ist aber auch in die Zukunft gerichtet: Das geplante europäische Notrufsystem „e-Call“ wird in der Praxis beweisen müssen, dass es wirklich datenschutzfreundlich umgesetzt ist.



Die Laudatoren der BigbrotherAwards 2014 von links nach rechts: Dr. Rolf Gössner (Internationale Liga für Menschenrechte), Prof. Dr. Peter Wedde (Professor für Arbeitsrecht und Recht der Informationsgesellschaft), Frank Rosengart (Chaos Computer Club e.V.), Rena Tangens (Digitalcourage e.V.), Sönke Hilbrans (Deutsche Vereinigung für Datenschutz e.V.), Prof. Dr. Martin Haase (Professor für romanische Sprachwissenschaft an der Universität Bamberg), padeluun (Digitalcourage e.V.), Dr. Heribert Prantl (Leiter des Ressorts für Innenpolitik bei der Süddeutschen Zeitung)

### Wirtschaft: CSC (Computer Sciences Corporation)

Der BigBrotherAward in der Kategorie Wirtschaft geht an die Firma CSC (Computer Sciences Corporation). Der Konzern arbeitet im Auftrag von 10 Bundesministerien an sicherheitsrelevanten Projekten wie dem elektronischen Personalausweis, der Kommunikation mit Behörden De-Mail und dem bundesweiten Waffenregister. Gleichzeitig ist die Mutterfirma die externe EDV-Abteilung der US-amerikanischen Geheimdienste und hat Entführungsflüge in Foltergefängnisse im Auftrag der CIA organisiert.

### Neusprech: Metadaten

In Gesprächen können wir viel verraten. Wirklich nackt aber machen uns erst unsere „Metadaten“. Sie verraten, was wir denken, planen und tun. Ein Beitrag von Kai Biermann und Martin Haase.

### Tadelnde Erwähnungen:

Debeka, Contipark, Kirchensteuer auf Abgeltungsteuer, WhatsApp, Talents-4Good, Telefon-Mitschnitte und ihre öffentliche Wahrnehmung

### Arbeitswelt: RWE Vertrieb AG

Der BigBrotherAward in der Kategorie Arbeitswelt geht an die RWE Vertrieb AG. Diese lässt in Call-Centern bei Subunternehmern eine Überwachungssoftware von Verint Systems einsetzen. Diese Software kann ohne das Wissen der Mitarbeiter im Einzelfall sowohl das Telefonat als auch Bildschirmaktionen aufzeichnen. Der Preis wird stellvertretend für alle Unternehmen vergeben, die sich technischer Aufzeichnungsmethoden zur Bewertung der Mitarbeiterinnen und Mitarbeiter in Call-Centern bedienen. Nur nebenbei: Verint Systems produziert auch Abhörtechnik für Geheimdienste, beispielsweise für die NSA.

### Verbraucherschutz: Die Firma LG

Die Firma LG bekommt einen BigBrotherAward in der Kategorie Verbraucherschutz, weil die von ihr verkauften „smarten“ Fernsehgeräte via Internetanschluss detaillierte Informationen über das, was sich die Menschen damit angesehen haben, an die Firmenzentrale nach Südkorea übermittelten. Anhand dieser Informationen, so genannter Metadaten, lassen sich intime Details über einzelne Menschen erfahren. Die LG-Geräte sind so in den privaten Lebensbereich argloser Menschen eingedrungen.

### Julia-und-Winston-Award (Positivpreis): Edward Snowden

In diesem Jahr wurde zum ersten Mal einen Positivpreis verliehen. Der „Julia-und-Winston-Award“ wurde benannt nach den „rebellischen“ Hauptcharakteren aus George Orwells dystopischem Roman „1984“, aus dem auch der „Große Bruder“ stammt. Der Award soll Personen auszeichnen, die sich in besonderem Maße gegen Überwachung und Datensammelwut eingesetzt haben. Der Preis ist auf eine Million dotiert – allerdings nicht eine Million Euro. Die Laudatio für den ersten Julia-und-Winston-Award hielt Heribert Prantl, Mitglied der Chefredaktion der Süddeutschen Zeitung.

# Datenschutznachrichten

## Datenschutznachrichten aus Deutschland

Bundesweit

### Kontodatenabfragen nehmen stark zu

Nach Angaben des Bundesfinanzministeriums durchleuchten staatliche Stellen private Konten so oft wie noch nie. 2013 verzeichnete das zuständige Bundeszentralamt für Steuern demnach knapp 142.000 dieser Kontenabfragen. Sie haben sich damit im Vergleich zu 2012 fast verdoppelt. Die Zahl der Abfragen 2012 (72.578) lag 15,5% über dem Vorjahr 2011 (DANA 1/2013, 17). Im ersten Quartal von 2014 wuchs die Zahl dem Bericht zufolge ähnlich stark - von gut 24.000 auf mehr als 48.000. Der nun erfolgte massive Zuwachs ist darauf zurückzuführen, dass neuerdings auch Gerichtsvollzieher prüfen dürfen, wer über welche Konten oder Wertpapierdepots verfügt.

Eingeführt wurden die Kontodatenabfragen erstmals zur Terrorismusbekämpfung im Jahr 2003. Seit 2005 haben Finanzämter und Sozialleistungsträger (Jobcenter, Ämter, die für BAFöG, Hartz-IV, Sozialhilfe od. Wohngeld zuständig sind) die Möglichkeit, online Kontodaten abzufragen, um zum Beispiel Sozialbetrüger oder Bürger, die Steuern hinterziehen, zu ertappen. Beauskunftet werden Name, Geburtsdatum, Adresse und Kontonummer des Bankkunden, nicht aber der Kontostand oder Kontobewegungen.

Die Zahl dieser Anfragen hat jedes Jahr kontinuierlich zugenommen. 2013 fragten Steuerbehörden in fast 69.000 Fällen Kontodaten ab - 7.000 mehr als 2012. Bei den Kontoabrufen der anderen Behörden ist der Anstieg in den vergangenen 15 Monaten nach Angaben des Finanzministeriums „nahezu vollständig“ auf die Gerichtsvollzieher zurückzuführen, die seit Anfang 2013 Auskünfte bei der Rentenversicherung, beim Bundeszentralamt für Steuern und beim Kraftfahrt-Bundesamt über Arbeitsverhältnisse, Konten und Fahrzeuge einholen dürfen, wenn sich die Ansprüche des Gläubigers auf mehr als 500 Euro belaufen. Dieses Instrument werde, so Detlef Hüermann, Bundesgeschäftsführer des Deutschen Gerichtsvollzieherbunds, vor allem bei unkooperativen Schuldnern genutzt, die keine Vermögensauskunft vorgelegt haben.

Die neue Bundesdatenschutzbeauftragte Andrea Voßhoff sieht die amtliche Neugierde kritisch. Prüfungen der Aufsichtsbehörden hätten ergeben, dass oft sogar die Begründungen für den konkreten Abruf fehlten und die Betroffenen nicht benachrichtigt werden. Sie sieht den Gesetzgeber deshalb „in der Pflicht, die Befugnis zum Kontenabruf zu überprüfen und auf das unbedingt erforderliche Maß zurückführen“. Dies gelte für die „Anzahl der Abfragen und auch den Umfang der abgefragten Datenmenge.“ Der Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein Thilo Weichert forderte, die Betroffenen nach erfolgter Abfrage zu unterrichten. Die Kontrollmöglichkeit durch die Betroffenen könne eine erzieherische Wirkung auf die Sachbearbeiter haben, keine unberechtigten Abfragen vorzunehmen. Dass dies faktisch nicht realisiert wird, wurde vom Bundesverfassungsgericht in einer Entscheidung vom 13.06.2017 nicht stärker problematisiert (Az. 1 BvR 1550/03 u. a.).

Bei der Finanzaufsicht Bafin hatten sich die Kontenabfragen zuletzt auch erhöht. Sie kletterten 2013 um sieben Prozent auf 122.664. Bislang gab es 2014 ebenfalls einen leichten Anstieg. Die meisten Anfragen, die bei der Bafin nur aufgrund strafrechtlicher Ermittlungen möglich sind, stammten von Polizei und Staatsanwaltschaften (Öchsner, Immer mehr Kontoabfragen durch Behörden, SZ 25.04.2014, 1).

Bund

### PPI-Studie zum CoC bei Versicherungen

In einer Studie „Code of Conduct Datenschutz Versicherungen“ des Software- und Beratungshauses PPI AG werden die Ergebnisse einer repräsentativen Befragung bei 60 Assekuranzen in Deutschland zu den von den Datenschutzaufsichtsbehörden und am 02.12.2012 vom Berliner Datenschutzbeauftragten förmlich anerkannten Verhaltensregeln nach § 38a BDSG (Code of Conduct - CoC) im Bereich der Versicherungswirtschaft dargestellt. Die Befragung erfolgte im Oktober 2013 bei Fach- und Führungskräften aus den Bereichen Compliance, Datenschutz, Marketing, Recht, Betriebsorganisation und IT (siehe auch DANA 2/2013, 62).

In 11 Leitsätzen und 31 Artikeln regelt der „Code of Conduct Datenschutz“ des Gesamtverbands der Deutschen Versicherungswirtschaft (GDV) die Erhebung, Verarbeitung, Speicherung und Nutzung von personenbezogenen Daten. Der CoC berührt sämtliche Bereiche und Sparten der Versicherungsunternehmen; ausgenommen ist nur die im PKV organisierte private Krankenversicherung. Gemäß den Angaben des GDV waren Anfang 2014 mehr als 260 Unternehmen beigetreten, die rund 80% des Marktes vertreten. Das Regelwerk entstand in enger Kooperation des GDV, von Unternehmensvertretern, den Datenschutzbehörden und der Verbraucherzentrale Bundesverband. Versicherer, die der freiwilligen Selbstverpflichtung beitreten, müssen ein umfassendes Datenschutz- und Datensicherheitskonzept vorweisen. Sie verpflichten sich, ihren Umgang mit personenbezogenen Daten für Datenschutzbehörden und Kundschaft transparent und besser nachprüfbar zu machen, vertrauenswürdig mit den Daten umzugehen und den Grundsatz der Datensparsamkeit zu beachten. Alle Produkte, Dokumente, Prozesse, Schnitt-

stellen, Vertriebswege und IT-Verfahren müssen hinsichtlich des Datenschutzes durchleuchtet werden.

Tobias Kohl, Studienleiter und Leiter Versicherungsbetrieb bei der PPI AG erläutert: „Wer den CoC Datenschutz unterschrieben hat, muss einen hohen Aufwand für die Umsetzung in Kauf nehmen, was einige Assekuranzen als große Herausforderung empfinden“. 66% der CoC-Teilnehmer schätzen das Risiko hoch beziehungsweise sehr hoch ein, dass die Kosten für die CoC-Umsetzung höher ausfallen können als geplant. 64% befürchten zudem, dass eine falsche Auslegung der CoC-Richtlinien zu falschen Entscheidungen führt. 54% der Versicherer sehen zudem die Gefahr, dass sie die Frist der CoC-Einführung nicht einhalten können. Innerhalb von zwei Jahren nach dem Beitrittsdatum müssen alle technischen Auflagen des CoC umgesetzt sein. 44% argwöhnen, dass konkrete Umsetzungsmaßnahmen nicht richtig festgelegt werden. 42% gehen davon aus, dass die Akzeptanz bei den Mitarbeitenden fehlt.

Diese Bedenken bestehen bei Versicherungsunternehmen, die dem COC bereits beigetreten sind. Insbesondere IT-Abteilungen schätzen die Risiken der Umsetzung hoch ein im Vergleich zu den etwas optimistischer gestimmten Fachabteilungen. Versicherer, die den CoC-Beitritt erst noch planen, zeigen sich eher zuversichtlich. Insbesondere die Vielzahl und Anzahl der Sparten, Produkte und Dokumente innerhalb eines Versicherungsunternehmens erhöhen den Aufwand der CoC-Einführung. Wegen der Heterogenität der IT-Landschaften sind durch den neuen Datenschutzkodex zahlreiche Änderungen in den IT-Verfahren nötig. Kohl: „Bei allen Herausforderungen sollten Versicherer stets an die Außensicht denken. Denn letztendlich wollen Kunden sich künftig darauf verlassen, dass die Abläufe ihres Versicherers regelkonform sind und ihr Bedürfnis nach Schutz der persönlichen Daten ernst genommen wird. Das so gestärkte Kundenvertrauen ist ein entscheidender Wettbewerbsvorteil für alle beigetretenen Assekuranzen.“

Dem gemäß sehen die Unternehmen trotz der mit der Einführung verbundenen Probleme den CoC positiv: 90% aller Versicherungsunternehmen schätzen grundsätzlich das Potenzial des CoC, mit der Selbstverpflichtung zu einem positiveren Bild in der Versicherungsbranche beizutragen als hoch bzw. sehr hoch ein. Nahezu ebenso viele Unternehmen versprechen sich davon eine Verbesserung des eigenen Images. Mehr als jedes zweite beigetretene Unternehmen hatte bereits seine Kundschaft über die Selbstverpflichtung informiert. 84% ist es wichtig, mithilfe des CoC-Beitritts das Kundenvertrauen zu steigern. Sachlich nicht ganz korrekt - es wurde ein Regelwerk zertifiziert, nicht die konkrete Datenverarbeitung - erläuterte Kohl: „Auf Kunden wirkt so ein umfassendes, zeitlich befristetes, unabhängiges Siegel durchaus vertrauenserweckend. Denn sie können sich darauf verlassen, dass die Abläufe ihres Versicherers künftig regelkonform sind und ihr Bedürfnis nach Schutz der persönlichen Daten ernst genommen wird.“ In der anhaltenden Niedrigzinsphase hätten Versicherungsunternehmen viel Kundenvertrauen eingebüßt. Der Beitritt zum CoC und die daraus resultierenden Modernisierungsmaßnahmen könnten zum entscheidenden Erfolgsfaktor in verschärften Wettbewerb werden: 73% der beigetretenen Versicherer wollen parallel zur CoC-Umsetzung die Verteilung der kundenbezogenen Informationen in der IT optimieren. 64% ist es wichtig, auch die Prozessdokumentation zu verbessern. 62% von ihnen planen, kundenbezogene Geschäftsvorfälle zu standardisieren. 40% wollen das Testmanagement angehen. 36% gaben an, sich künftig vornehmlich dem Aufbau der Facharchitektur zu widmen. Der CoC ist im Internet verfügbar unter http://www.gdv.de/wp-content/uploads/2013/03/GDV_Code-of-Conduct_Datenschutz_2012.pdf (Studie zum Code of Conduct in der Versicherungswirtschaft, PPI Forum, April 2014, S. 6; GDV - Die Positionen der deutschen Versicherer 2014, S. 22; Neuer Datenschutzkodex: Zwei Drittel der Versicherer fürchten hohe Umsetzungskosten, www.presseportal.de 04.03.2014).

Baden-Württemberg

## Lebensversicherung informiert Kunden übermäßig

Als ein Kunde der Württembergischen Lebensversicherung, die zur Wüstenrot-Gruppe gehört, Informationen zu seiner fondsgebundenen Lebensversicherung anforderte, wunderte er sich über die Antwort: Er erhielt ein dickes Paket zugesandt, das Kopien von rund 150 Briefen, Standmitteilungen und Mahnschreiben an etliche Versicherte des Unternehmens enthielt, die anscheinend gleiche oder ähnliche Produkte gekauft hatten wie der Kunde. Das Unternehmen erklärte, dass es prüfe, „ob es sich um ein reines Versehen oder um einen technischen Fehler im Versandprozess handelt“, und versprach eine „Optimierung unserer Versandabläufe, um nachhaltig sicherzustellen, dass sich solche Vorgänge nicht wiederholen“ (Der Spiegel 14/2014, 63).

Bayern

## Bürgermeister verurteilt wegen intimer Fotos

Ein inzwischen suspendierter Bürgermeister der Gemeinde Scheyern im Landkreis Pfaffenhofen wurde am 11.03.2014 vom Amtsgericht (AG) München wegen Beleidigung, Widerstands gegen Vollstreckungsbeamte und vorsätzlicher Körperverletzung zu einer Geldstrafe von 75 Tagessätzen zu 70 Euro verurteilt. Das AG sah es als erwiesen an, das der 56jährige Kommunalpolitiker im Juni 2013 am Münchner Stachus auf einer Rolltreppe Frauen unter den Rock fotografiert hatte. Der Mann konnte nur wegen eines Falles verurteilt werden, weil dies nur eine Frau bemerkt und ihn angezeigt hatte. Die Polizei stellte den Mann und stellte auf der Speicherkarte seiner Digitalkamera 27 Filme und 99 verfängliche Fotos fest. Der Mann hatte sich gegen die Festnahme gewehrt und einem Beamten seinen Ellenbogen in den Bauch gerammt. Der frühere Bürgermeister war damit nicht zum ersten Mal mit Spannervorwürfen konfrontiert. Anfang 2009 soll er auf einer Damentoilette an der Autobahn 9 einen Spiegel unter eine Kabinenwand hindurch gehalten und eine junge Frau beobachtet haben. Dabei hatte er - um nicht aufzufallen - eine Frauenperücke getragen. Der Verwaltungsgerichtshof befand im Dezember 2012 in letzter Instanz, dass die Sache mit dem Spiegel auf der Toilette nicht nachzuweisen sei

(Salch, Bürgermeister wegen Sex-Fotos verurteilt, SZ 12.03.2014, 30).

### Hessen

## Polizei bekommt Mini-Schulterkameras

Von Mai 2014 an sollen in einigen Vierteln der Städte Wiesbaden und Offenbach, in denen es öfter mal Randale gibt, Ordnungshüter mit sogenannten Körperkameras - kurz Body-Cams - ausgestattet werden. Dabei handelt es sich um Videokameras, die auf der Schulter der Uniformweste angebracht sind und die dem Schutz der Beamten vor Übergriffen dienen sollen. Zuvor wurde diese Technik erstmalig im Frankfurter Kneipenviertel in Sachsenhausen und in der Fußgängerzone Zeil erprobt. Die Ergebnisse haben sowohl Politik wie auch Polizei überzeugt. Landesinnenminister Peter Beuth (CDU) verkündete die Ausweitung des seit Mai 2013 laufenden Pilotprojekts, nachdem sich die Erwartungen der Sicherheitsfachleute - eine „deeskalierende und präventive Wirkung" - eingestellt hätten. Im zweiten Halbjahr 2012 habe man an den beiden Frankfurter Orten noch 27 Übergriffe auf Beamte gezählt, von Juni bis November 2013 nur noch 20. Anders als früher sei dort kein Polizist mehr verletzt worden. Allein die Existenz der Kameras sorge dafür, dass Störenfriede nicht mehr so ruppig seien.

Die Grünen, CDU-Juniorpartner in der Landesregierung und gemeinhin skeptisch gegenüber Formen technischer Überwachung, haben gegen die Body-Cams ebenso nichts einzuwenden wie der Hessische Datenschutzbeauftragte (HDSB). Klare Regeln sollen einen Missbrauch verhindern: Die Kamera wird nur in brenzligen Situationen eingeschaltet; Tonaufnahmen sind verboten; die Betroffenen sollen auf das Gerät hingewiesen werden. Irrelevantes Material muss nach dem Einsatz vernichtet werden. Wenn es Probleme gab, dürfen die Polizisten die Filme für maximal sechs Monate aufbewahren. Verstöße gegen diese Vorschriften seien bislang nicht bekannt, sagte Barbara Dembowski, beim HDSB zuständig für Polizeifragen.

Andere Bundesländer verfolgen das hessische Pilotprojekt mit Interesse. Hamburg findet die Kameras gut; in Bayern wird gerade geprüft, ob die Kameras im Kampf gegen Gewalt an Polizisten hilfreich sein könnten und ob das Polizeirecht solche Videoaufnahmen erlaubt. In Nordrhein-Westfalen und anderswo ist man eher skeptisch. Es besteht die Sorge, dass die Aufnahmen zur Überwachung der Beamten und zu deren Nachteil verwendet werden könnten. Befürchtet werden zudem massive Eingriffe in die Privatsphäre der Bürger und in das Vertrauen der Menschen in die Polizei. Der Vorsitzende der Gewerkschaft der Polizei (GdP) in Hessen, Andreas Grün erklärte, es habe bislang keinen einzigen Fall gegeben, in dem ein Beamter von seinem Vorgesetzten wegen Fehlverhaltens bei einem gefilmten Einsatz gerügt worden sei. Die Resultate des Pilotprojekts seien allesamt positiv. Wenn sich das herumspreche, würden auch anderswo Kameras eingesetzt werden, jedenfalls in Städten mit Problemzonen. Zugleich warnt Grün vor überzogenen Erwartungen: Ein Allheilmittel gegen die bundesweit wachsende Gewalt an Polizeibeamten seien die Kameras natürlich nicht (Höll, Filmreife Verbrechen, SZ 02.05.2014, 1).

# Datenschutznachrichten aus dem Ausland

### Europa

## Datensicherheitsmängel bei Krankenhäusern

Deutsche Krankenhäuser haben laut einer aktuellen Studie der Wirtschaftsberatungsgesellschaft Price Waterhouse Coopers (PwC) im Auftrag der Europäischen Kommission Schwächen bei der Sicherheit sensibler Patientendaten. Danach ist eine Verschlüsselung gespeicherter Patientendaten nur in 40% der deutschen Kliniken üblich. Damit liege Deutschland wenig über dem EU-Durchschnitt, aber deutlich unter anderem hinter Großbritannien, Finnland oder auch Rumänien. Der Zugang zum IT-System sei in Deutschland in der Regel nach Eingabe eines Passwortes möglich. Nur in jedem vierten Krankenhaus werden der Erhebung zufolge Daten zusätzlich durch eine sogenannte digitale Signatur geschützt. Gegen einen Systemausfall und einen drohenden Datenverlust sind laut der Studie viele Häuser nicht gewappnet. In Deutschland haben nur rund 80% der Kliniken eine Notfallstrategie; europaweit sind dies drei von vier Krankenhäusern. Lediglich 14% der europäischen und 20% der deutschen Krankenhäuser haben ein ausreichendes Datensicherungssystem zur sofortigen Wiederherstellung aller Informationen. In jeder dritten deutschen Klinik könnten Daten bei einem Systemausfall erst nach 24 Stunden wiederhergestellt werden.

Für die Studie wurden 1717 Akutkliniken in der EU sowie Norwegen und Island befragt. Aus Deutschland beteiligten sich 201 Krankenhäuser. Die Analyse zeigt, dass deutsche Krankenhäuser die Möglichkeiten der Digitalisierung bislang nur unzureichend nutzen. Insbesondere bei der elektronischen Übermittlung von Befunden, Patientenbriefen und Laborergebnissen an Ärzte oder Krankenkassen seien Kliniken in anderen Ländern weiter. Gut jede siebte deutsche Klinik der Akutversorgung hat überhaupt keine elektronische Patientenakte (Deutsche Krankenhäuser schwächeln bei Datensicherheit, www.handelsblatt.com 29.04.2014).

Europa

## EU und Brasilien planen gemeinsames Datenkabel

Am 24.02.2014 reiste die Präsidentin von Brasilien Dilma Rousseff nach Brüssel zu einem Gipfeltreffen mit der Europäischen Union (EU). Dort wurde neben vielen anderen Themen über ein gigantisches Glasfaserkabel zwischen Europa und Brasilien gesprochen, mit dem möglichst noch im Jahr 2014 begonnen werden soll. Die schon länger verfolgten Planungen haben gemäß hochrangigen EU-Beamten einen starken Schub erhalten, nachdem Europäern und Brasilianern bewusst wurde, wie sehr sie von den amerikanischen Nachrichtendiensten überwacht werden. So wurde das Telefon von Präsidentin Rousseff ähnlich wie das der deutschen Kanzlerin Angela Merkel bespitzelt. Aus Verärgerung darüber hatte Brasiliens Staatschefin unter anderem ein Treffen mit US-Präsident Barack Obama abgesagt.

Die Kommunikation zwischen Lateinamerika und Europa ist in vielfacher Hinsicht vergleichsweise anfällig. Es gibt nur eine einzige direkte, 8.500 Kilometer lange Telekommunikationsverbindung zwischen Europa und Brasilien von Lissabon nach Fortaleza im brasilianischen Nordosten mit dem Namen „Atlantis II“. Sie stammt aus dem Jahr 2000 und gilt als alt und überlastet, sodass sie nur für die Übertragung von fernmündlichen Gesprächen verwendet werden kann. Für den Internet-Datenverkehr ist sie nicht geeignet. Diese transatlantischen Verbindungen Brasiliens laufen über drei weitere Unterseekabel, die allesamt über die USA führen. Das ist unsicher und zudem langsamer und teurer als eine Direktverbindung. Deshalb hat die staatlich kontrollierte Fernmeldegesellschaft TeleBras zusammen mit dem spanischen Unternehmen Islalink ein Joint Venture gegründet, an dem sich bis Mitte 2014 weitere Firmen beteiligen sollen. Auch jenseits der brasilianischen Grenzen soll es Interesse geben, bei dem Projekt mitzumachen. Brasilien will auch seine Verbindungen ins kontinentale Hinterland verbessern.

In Brüssel ist zu hören, es werde intern geprüft, ob und in welchem Umfang sich die EU mit öffentlichem Geld an der Leitung beteiligt. EU-Ratspräsident Herman Van Rompuy unterstrich, dass der Cyberspace der Bereich sei, in dem die Zusammenarbeit zwischen Europa und Brasilien intensiviert werden solle - „damit wir die Vorzüge neuer Technologien sicher nutzen und ein freies und offenes Internet“ geschützt bleibe (Cáceres, Leitung ohne Lauscher, SZ 24.02.2014, 1).

Italien

## 1 Mio. Euro Strafe wegen Google Street View

Die italienische Datenschutzbehörde Garante per la protezione dei dati personali hat Google eine Strafe von einer Million Euro auferlegt wegen Datenschutzverstößen beim Aufnehmen der Straßenansichten für seinen Dienst Street View. Google hat die Strafe umgehend bezahlt. Die Datenschutzbehörde hatte Google im Jahr 2010 auferlegt, die Bevölkerung per Radiowerbung und Zeitungsanzeigen auf kommende Street-View-Aufnahmen hinzuweisen. Auch sollten die Google-Fahrzeuge deutlich markiert und damit als Aufnahmefahrzeuge erkennbar sein. Drei Tage vor den Aufnahmen sollte Google veröffentlichen, welchen Ort die Fahrzeuge befahren werden. So sollten sich die Menschen in den betroffenen Gebieten den Aufnahmen entziehen können. Das sei ihnen aber in vielen Fällen nicht möglich gewesen. Viele Menschen, die nicht wollten, dass Bilder von ihnen im Web veröffentlicht werden, hatten sich bei der Behörde beschwert.

Google hatte zuvor auch in anderen Ländern Ärger wegen Datenschutzverstößen im Zusammenhang mit seinem Dienst Street View. In Deutschland musste Google eine Geldbuße von 145.000 Euro zahlen, weil die Kamerafahrzeuge in den Jahren 2008 bis 2010 nicht nur Straßen und Häuser fotografiert, sondern auch die WLAN-Funknetze erfasst haben. Dabei haben die Fahrzeuge auch Inhaltsdaten unverschlüsselter Netze aufgezeichnet. In Frankreich wurden wegen des gleichen Vergehens 100.000 Euro fällig, in den USA 7 Millionen US-Dollar (5,4 Millionen Euro). Aktuell ermitteln europäische Datenschutzbehörden und verhängten schon Geldstrafen, weil Google Anfang März 2012 eine neue Datenschutzerklärung einführte, wonach sich der Konzern genehmigen lässt, persönliche Daten aus verschiedenen Diensten wie Google+, Picasa, Drive, Docs, Maps und andere miteinander zu kombinieren und weiterzuverwenden (Google Street View: Eine Million Euro Strafe in Italien wegen Verstoß gegen Datenschutz, www.heise.de 04.04.2014).

Brasilien

## Digitales Schutzgesetz „Marco Civil“

Zu den Objekten der Kommunikations-Dauerbeobachtung des US-amerikanischen Geheimdienstes National Security Agency (NSA) gehörte neben der deutschen Bundeskanzlerin Angela Merkel oder dem mexikanischen Präsidenten Enrique Pena Nieto auch die Präsidentin Brasiliens Dilma Rousseff. Umfassend ausspioniert wurde zudem ein Motor der brasilianischen Wirtschaft, der staatliche Ölkonzern Petrobas. Als eine Entschuldigung für diese Beobachtung ausblieb, sagte Rousseff einen vereinbarten Besuch bei US-Präsident Barack Obama einfach ab. Am 23.04.2014 unterschrieb Rousseff nun ein Gesetz, das den größtmöglichen Kontrast zu den USA markieren soll - eine Art Grundrechtekatalog für das von den USA dominierte Internet. Schon 2007 hatte die Regierung in Brasilia eine „nationale Verfassung“ für das Netz angeregt. Das nun vorgelegte „Marco Civil“ wurde binnen weniger Tage vom Parlament und Senat verbschiedet und von der Staatschefin unterzeichnet. Es verspricht den 200 Mio. Menschen in Brasilien Privatsphäre, Meinungsfreiheit, die Einhaltung von Bürgerrechten und Gleichheit im Netz. Daten müssen 6 Monate für Provider und ein Jahr für Websites gespeichert werden; Klagen werden von der Justiz angenommen. Rousseff erklärte, man müsse „die Rechte, die Menschen offline haben, auch online schützen“.

Die seit 2011 an der Spitze der sozialdemokratischen Regierung stehende Rousseff nutzte eine Rede auf der Weltkonferenz NETmundial am 23./24.04.2014 in Sao Paulo für eine digitale Großoffensive. Brasilien ist äußerst technologiefreundlich und nutzt - ebenso wie Deutschland - noch umfassend die IT-Angebote von US-Firmen wie Microsoft, Apple, Google, Facebook und Twitter. Das wohl wichtigste Sprachrohr von Edward Snowden, der ausgewanderte US-Reporter Glenn Greenwald, lebt und arbeitet in Rio de Janeiro. Brasilien plant ein eigenes Glasfaserkabel über den Atlantik, um die Internet-Knotenpunkte in den USA zu umgehen (s. o. Europa).

Der erste Entwurf für ein Internet-Reglement sah noch vor, dass ausländische Unternehmen wie Facebook Datenzentren in Brasilien haben sollten. Diese Vorgabe wurde in der finalen Fassung gestrichen. Geregelt ist, dass Firmen zwar unterschiedliche Bandbreiten bei der Datenübertragung verkaufen, aber keine Kundschaft bevorzugen oder deren Zugang beschränken dürfen. Die Gerichtsbarkeit gegen etwaige Verstöße auch fremder Anbieter unterliegt Brasilien. Rousseff erhält für ihren Vorstoß im Lande viel Beifall. In Facebook nannte sie das Marco Civil das „fortschrittlichste Gesetz der Welt“ (Burghardt, Brasilien wirbt für ein gerechteres Internet, SZ 26./27.04.2014, 8).

## USA

## CIA späht Kontrolleure aus

Dianne Feinstein, die 80jährige demokratische Vorsitzende des Geheimdienstausschusses im US-Senat, beschuldigte die CIA in einer dreiviertel Stunde dauernden Rede im Senat öffentlich, Senatscomputer durchsucht und Dateien gelöscht zu haben. Damit sei gegen Bundesgesetze verstoßen und die Gewaltenteilung, wie sie die US-Verfassung vorsieht, verletzt worden. Sie bestätigte damit am 11.03.2014 in weiten Teilen Medienberichte der vorangegangenen Woche über den Spähangriff des Nachrichtendienstes auf Kongressmitarbeiter. Die CIA habe Mitarbeiter von ihr bei der Bundespolizei FBI unter dem Verdacht des Geheimnisverrats angezeigt, also des Ausschusses, dessen Aufgabe es ist, die US-Geheimdienste einschließlich die CIA zu überwachen: „Ich habe die CIA um eine Entschuldigung gebeten, ich habe keine bekommen.“

In dem Fall geht es ursprünglich um eine Untersuchung von Foltervorwürfen gegen die CIA, die der Geheimdienstausschuss durchführen soll und dazu unter anderem Dokumente von der CIA anforderte. Auf offenbar noch geheimen 6.300 Seiten hat der Ausschuss die CIA-Exzesse von „erweiterten Verhörtechniken“, wie u. a. das sog. Waterboarding genannt wird, dokumentiert. Die CIA habe, so Feinstein, die Dokumente nicht herausgeben wollen, sondern darauf bestanden, dass nur vorkontrollierte Dateien auf Computern zugänglich gemacht werden, die in CIA-Anlagen stehen. Dort sollten sie dann von Kongressmitarbeitern gelesen werden. Es wurde ein Konvolut von 6,2 Mio. Dateien auf die separaten Computer überspielt. Darunter war auch ein interner CIA-Bericht, der die schlimmsten Vorwürfe bestätigte, die Feinstein aber nicht näher beschrieb, weil sie noch der Geheimhaltung unterliegen.

Bald sei jedoch aufgefallen, dass Dokumente von diesen Rechnern wieder verschwanden, obwohl die CIA dazu keinen Zugang haben sollte. Der Nachrichtendienst selbst habe erst erklärt, man sei nicht verantwortlich, sondern die externen Mitarbeiter, die zur Administration der Technik angestellt worden waren. Später habe man sich auf eine Verfügung des US-Präsidenten berufen, das sei aber vom Weißen Haus dementiert worden. Anfang 2014 hackte die CIA die Senatscomputer ein zweites Mal, offenbar um den besonders inkriminierenden Bericht zu löschen. Feinsteins Mitarbeiter hatten aber eine Kopie angefertigt und diese in einem Safe deponiert. Die CIA warf ihnen deshalb vor, ihre Geheimhaltungspflichten verletzt zu haben. Lange habe sie versucht, diese Vorwürfe diskret zu klären, aber das sei nun nicht mehr möglich, erklärte Feinstein.

Feinstein scheint als Hauptverantwortlichen für das Vorgehen der CIA deren obersten Rechtsberater Robert Eatinger ausgemacht zu haben, der den vermeintlichen Datendiebstahl von Feinsteins Mitarbeiter beim FBI gemeldet hatte. Eatinger war Anfang des vergangenen Jahrzehnts bereits in der Rechtsabteilung des CIA tätig und hatte dort das CIA-Verhörprogramm gebilligt. Eatingers jetziger Chef John Brennan war damals Leiter des Antiterror-Centers der CIA und wurde 2008 zum Antiterrorberater Barack Obamas. Nach dessen Wahl sollte er bereits 2009 CIA-Direktor werden, was aber damals an seiner Verwicklung in das Verhörprogramm scheiterte. 2013 machte ihn Obama dann doch zum CIA-Direktor.

Feinstein berichtete, dass der erstellte Report über die Misshandlung von Terrorverdächtigen durch die CIA inzwischen an US-Präsident Obama übersandt wurde. Dieser solle dafür sorgen, dass die Geheimhaltung aufgehoben werde, damit die „schrecklichen Details eines CIA-Programms, das niemals hätte existieren dürfen“, öffentlich würden. Der jetzige CIA-Direktor Brennan wies die Vorwürfe Feinsteins umgehend zurück. Man schulde es den „Frauen und Männern in der CIA, die treu ihre Pflicht getan haben“, dass alle Fakten „ausgewogen und akkurat“ wiedergegeben würden (Klüver, Angriff auf die Kontrolleure, SZ 13.03.2014, 9; US-Senatorin erhebt schwere Vorwürfe gegen die CIA, www.heise.de 11.03.2014).

Jetzt DVD-Mitglied werden:
www.datenschutzverein.de

# Technik-Nachrichten

## Kontaktlinse misst Blutzuckerwert

Das Forschungslabor Google X hat eine digitale Kontaktlinse für Diabetiker entwickelt, die über die Tränenflüssigkeit den Blutzucker-Wert eines Menschen misst. Die EntwicklerInnen stellten die Linse, die sich noch in einem frühen Entwicklungsstadium befindet, in ihrem Blog vor. Der Prototyp besteht aus zwei herkömmlichen weichen Kontaktlinsen, zwischen denen ein Sensor sowie ein Miniatur-Funkchip eingebettet sind. Chip und Sensor sind so klein wie Glitzer-Partikel; die Funk-Antenne ist dünner als ein menschliches Haar. Mithilfe der verbauten Technik misst die Linse sekündlich die Glucose-Werte in der Tränen-Flüssigkeit und soll dann die Daten an eine begleitende Smartphone-App funken. Die Forschenden denken darüber nach, Mikro-LED-Lämpchen direkt in die Linse zu integrieren: Fällt der Wert über einen kritischen Wert, könnte ein Blinken die Kontaktlinsenträger warnen.

Schon seit längerem ist bekannt, das sich über die Tränenflüssigkeit der Blutzuckerspiegel messen lässt. Allerdings gelang es Forschern der University of Michigan erst im September 2011, eine verlässliche Messmethode zu finden. Im Fachmagazin Analytical Chemistry stellten sie einen nadelförmigen Chip fürs Auge vor, der ebenfalls den Blutzuckergehalt über die Tränenflüssigkeit misst. In einem Test mit Hasen zeigten die WissenschaftlerInnen, dass ihre Methode genauso zuverlässig ist wie das klassische Piksen in den Finger, das bislang für die Messung des Blutzuckerspiegels genutzt wird. Einen Monat später zog ein Forschungsteam der University of Washington gemeinsam mit Microsoft nach. Statt in einer Miniaturnadel war ihr Chip in einer Kontaktlinse verarbeitet. Ein fertiges Produkt ist daraus aber bisher nicht geworden. Ende 2012 stellten auch Forschende des Fraunhofer-Instituts für Mikroelektronische Schaltungen und Systeme einen Diabetes-Chip für das Auge vor. Einer der damals an dem US-Projekt beteiligten Forschenden war Babak Parviz, der mittlerweile bei Google angestellt ist und neben der Datenbrille Google Glass auch die jetzt vorgestellte Kontaktlinse mitentwickelt hat.

Derzeit müssen DiabetikerInnen sich jeden Tag mehrmals in den Finger stechen, um ihren Blutzucker zu messen. Das ist nicht nur schmerzhaft und vor allem in den Anfangsjahren nach der Diabetes-Diagnose eine Qual. In manchen Fällen können sich Entzündungen und Verhornungen an der Einstichstelle bilden. Eine permanente Messung über die Tränenflüssigkeit wäre also präziser, gesünder und vor allem schmerzfrei. Die Forschenden erklärten, es sei noch viel zu tun, bis die Kontaktlinse auf den Markt kommen könne. Google wolle sich dafür in dem Bereich erfahrene Partner suchen, die Zugang zu der Technologie bekämen (Google entwickelt Kontaktlinse für Diabetiker, www.zeit.de 17.01.2014).

## Patentantrag für Kontaktlinse mit Kamera

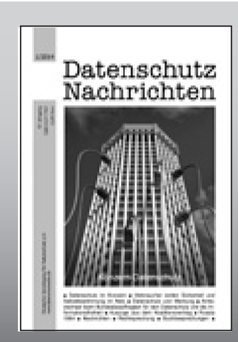
Google hat beim US-amerikanischen Patentamt einen Patentantrag eingereicht, in dem sich das Unternehmen eine Kontaktlinse mit Kamera und Display schützen lassen will. In die vom Forschungslabor Google X ausgedachte Kontaktlinse ist eine Kamera eingebaut, die über einen ebenfalls eingebauten Sensor durch einen Lidschlag ausgelöst werden kann. Die Kontaktlinse soll die Daten an ein Gerät wie ein Mobiltelefon senden können, damit dort die Bilder ausgewertet und gespeichert werden. Der Antrag auf ein „Image Capture Component on Active Contact Lens“ wurde im Oktober 2012 eingereicht und im April 2014 veröffentlicht. Mit Hilfe der Kamera soll der Träger u. a. sein Gesichtsfeld erweitern können. Die Bilder aus der Peripherie könnten über ein ebenfalls in die Kontaktlinse eingebautes Display angezeigt werden. Sehbehinderte könnten von der Technik profitieren, z. B. könnte die Kamera die Situation an einem Fußgängerüberweg filmen, die Bilder an ein Smartphone senden, das sie auswertet und den Kontaktlinsenträger warnt, falls sich ein Auto nähert. Den nötigen Strom könne ein Akku oder auch ein Solarelement liefern (Google will Kontaktlinse mit eingebauter Kamera patentieren lassen, www.heise.de 16.04.2014).












online zu bestellen unter: **www.datenschutzverein.de**

# Soziale Medien



## Facebook-Gesichtserkennung – fast so exakt wie das menschliche Auge

Die in der Entwicklung befindliche Facebook-Gesichtserkennungssoftware Deepface kann mittlerweile Gesichter fast so gut erkennen wie der Mensch. Bei einem Standardtest erreichte sie eine Genauigkeit von 97,25 Prozent, was beinahe den menschlichen Fähigkeiten entspricht. Menschen bringen es auf eine Genauigkeit von 97,53 Prozent.

Die Software kann selbst solche Gesichter erkennen, die schlecht beleuchtet oder aus einem ungünstigen Winkel aufgenommen sind. Deepface korrigiert hierfür im ersten Schritt den Kamerawinkel in einem 3D-Modell. Es können so nicht nur frontale, sondern auch seitliche Ansichten des Gesichts erstellt werden. Die Software errechnet dann mittels neuronaler Netze eine numerische Repräsentation der Gesichtsmerkmale.

Die Implementierung von Deepface in Facebook ist bislang noch nicht geplant. Der Konzern stellt die Forschungsergebnisse erstmals im Juni auf der IEEE Conference on Computer Vision and Pattern Recognitions in Ohio vor. (Facebook-Software erkennt Gesichter fast so gut wie ein Mensch, www.abendzeitung-muenchen.de 19.03.2014; André Kramer, Facebook unterscheidet Gesichter auf menschlichem Niveau, www.heise.de, 18.03.2014)

## Facebook schluckt WhatsApp – Datenschützer Thilo Weichert warnt die Nutzer

Angesichts des Kaufs von WhatsApp durch den Internetgiganten Facebook, warnt der Schleswig-Holsteinische Datenschutzbeauftragte Thilo Weichert vor einer Nutzung dieser Online-Dienste. „Wem die Vertraulichkeit der eigenen Kommunikation etwas wert ist, der sollte auf vertrauenswürdige Dienste zurückgreifen“, sagte Weichert Mitte Februar in einem vom Schleswig Holsteinischen Zeitungsverlag veröffentlichtem Interview. Er riet zu Diensten mit einer Ende-zu-Ende-Verschlüsselung. Aus Sicht des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein ist zu befürchten, dass die Kommunikationsmetadaten und -inhalte der beiden Dienste durch den Betreiber zusammengeführt werden, zur Profilbildung genutzt und für Werbezwecke missbraucht werden könnten. In den USA gibt es keine Gesetze, die die Zusammenführung der Daten der beiden Dienste verbieten. (Datenschützer Weichert warnt vor Kombination Facebook/WhatsApp, www.shz.de, 20.02.2014; Mira Nagar, Weichert: „Am schlimmsten ist die Kombination“, www.shz.de, 20.02.2014)

## Start-up Datacoup kauft Nutzern Social Media Daten ab – für 8 Dollar im Monat

Das amerikanische Start-up Datacoup will Nutzern von Social Networks bis zu acht Dollar im Monat für ihre Daten zahlen. Je mehr Daten freigegeben werden, umso mehr Geld kann der Nutzer erhalten. Das Unternehmen hat einen Betatest gestartet, an dem im März bereits 1.500 Nutzer teilnahmen. Die Nutzer erteilen Datacoup Zugriff zu ihren Facebook- und Twitterdaten sowie ihren Kreditkartenabrechnungen. Datacoup errechnet hieraus Trends und will diese anschließend an die Wirtschaft verkaufen. Die Daten werden nach Aussage des Geschäftsführers Matt Hogan ausschließlich anonymisiert verarbeitet. Zukünftig sollen auch weitere Datenquellen wie z. B. der Browserverlauf oder Daten aus Lifelogging-Geräten wie dem FitBit-Armband genutzt werden.

Bislang hat Datacoup noch keine Daten an Werbevermarkter verkauft. Die bisherigen Gespräche seien jedoch ermutigend gewesen, versichert Matt Hogan. Neu sei, dass Datacoup Daten aus Onlineverhalten und Kreditkartenverkäufen kombinieren kann. „Beide Datenquellen sind für sich genommen schon wertvoll“, sagt Hogan. „Wenn Sie beide übereinander legen, können Sie noch mehr Wert generieren. Aber das geht nur, wenn der Nutzer selbst das zulässt.“ Datacoup hat im Rahmen des Betatests jedoch bereits festgestellt, dass die meisten Nutzer weit weniger als acht Dollar im Monat einnehmen. Der Durchschnitt im Februar lag bei 1,56 Dollar. Hogan sagt hierzu: „Selbst wenn ich nur einen Dollar bekomme, ist dies immer noch mehr als das was ich derzeit bekomme.“ Fraglich ist allerdings, ob Nutzer bereit sein werden, ihre Daten für ein paar Cents zu verkaufen. (Tom Simonite, Der Marktwert der Verbraucherdaten, www.heise.de, 19.02.2014; Ben Schwan, Accountdaten gegen Geld: Datacoup will sich Nutzerdaten erkaufen, www.heise.de, 19.02.2014; Adam Tanner, Others take your data for free, this site pays cash, www.forbes.com, 03.03.2014)

## Facebook startet Datenschutz-Informationsportal

Die neue Facebook-Seite heißt „Leben in einer vernetzten Welt“ (www.aconnectedlife.info). Sie soll Nutzer informieren, wie sie ihre personenbezogenen Daten im Internet schützen können. Das Portal gibt zum einen Tipps zu den Privatsphäre-Einstellungen von

Facebook. Zum anderen wird darüber informiert, wie User nutzungsbasierte Online-Werbung im Internet abschalten können.

Für Markus Beckedahl enthält diese Seite eine Menge Ironie. Laut der Seite solle der Nutzer nicht zögern zu fragen, welche Daten über ihn gesammelt werden, wie diese verwendet werden und wer diese sehen kann. Beckedahl meint dazu: „Wir würden uns freuen, wenn diese Fragen von Facebook zur Datenverarbeitung bei Facebook auch beantwortet werden, aber bisher haben wir die Antworten noch nicht gefunden. Stattdessen wird auf den eigenen Support verwiesen. Oder aber an den irischen Datenschutzbeauftragten."

Tatsächlich weist Facebook auf www.aconnectedlife.info darauf hin, dass sich der Nutzer an die zuständige Datenschutzaufsichtsbehörde wenden kann, wenn sich ein Problem nicht mit dem Unternehmen oder über einen vertrauenswürdigen Dritten lösen lässt. Facebook informiert, dass die für das Unternehmen zuständige Behörde der Data Protection Commissioner of Ireland ist. „Wenn du spezifische Fragen zu deinen Daten und Facebook hast, kannst du dich also auch über die Website oder per E-Mail (info@dataprotection.ie) an den irischen Datenschutzbeauftragten wenden." heißt es auf den neuen Datenschutz-Informationsseiten. Leider hat der irische Datenschutzbeauftragte nur wenige Ressourcen. Daher kann er sich um Facebook und die diversen anderen US-amerikanischen Großunternehmen, für die er zuständig ist, kaum angemessen kümmern.

Auch innerhalb seines Dienstes hat das Unternehmen Neuerungen in Sachen Datenschutz geplant, um sein Datenschutz-Image aufzupolieren. In den USA sensibilisiert nun ein Assistent in Form eines blauen Dinosauriers die Nutzer für ihre Privatsphäre-Einstellungen. Er erscheint immer dann, wenn Nutzer sehr viele Informationen öffentlich teilen und diese Einstellung länger nicht geändert haben. „Wir testen ununterbrochen neue Wege, um sicherzustellen, dass die Leute entscheiden können, wer ihre Inhalte sehen kann.", sagt eine Facebook-Pressesprecherin. Derzeit gibt es den Dino nur in den USA, es sei jedoch auch denkbar, dass es in Deutschland getestet wird. (Jo Bager, Facebook eröffnet Datenschutz-Portal, www.heise.de, 11.04.2014; Hilfe vom Datenschutz-Dino, www.sueddeutsche.de, 02.04.2014; Markus Beckedahl, Facebook startet Datenschutz-Aufklärungs-Simulation, www.netzpolitik.org, 11.04.2014)

## Private Facebook-Öffentlichkeitsfahndung von Juwelier

Ein Juwelier aus Fürth veröffentlichte auf seiner Facebook-Fanpage Bilder und einen Ausschnitt aus Aufnahmen seiner Videoüberwachung, die zwei Täter eines Raubüberfalls vom 14.03.2014 zeigten. Von einer Journalistin darauf hingewiesen, wandte sich das Bayerische Landesamt für Datenschutzaufsicht in Ansbach (BayLDA) an den Juwelier und legte ihm telefonisch die Löschung der Veröffentlichung nahe. Dieser bedanke sich für den rechtlichen Hinweis und die Beratung „auf dem kleinen Dienstweg" und sagte die Löschung zu. Auf seinem Facebook-Account verwies er mit Link „direkt auf die Homepage der Polizei", wo nun neben weiteren Informationen die Fotos und Videos zu finden seien.

Das BayLDA nahm den Fall zum Anlass, per Presseerklärung darauf hinzuweisen, dass mit einem Hochladen von derartigen Bildern bei Facebook gemäß den Geschäftsbedingungen dieses Werbeportals „alle Rechte an der weiteren Nutzung dieser Bilder auf Facebook ... übertragen" werde. Aus diesem Grund veröffentliche auch die Bayerische Polizei keine Fahndungsbilder mehr auf Facebook. Das BayLDA warnt vor einer durch private Fahndungen in sozialen Netzwerken ausgelösten „Hetzjagd". In der Vergangenheit seien Fahndungsbilder direkt auf Facebook mit einem Aufruf zur Lynchjustiz verbunden gewesen. Es wies darauf hin, dass die 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung „Öffentlichkeitsfahndung der Strafverfolgungsbehörden mit Hilfe sozialer Netzwerke" eine restriktive Praxis eingefordert hat, die dazu führt, dass auch für Strafverfolgungsbehörden wie die Polizei eine Öffentlichkeitsfahndung über Facebook ausscheidet. Weiter weist das BayLDA darauf hin, dass es in einem Rechtsstaat nicht die Aufgabe von Privaten und auch nicht von Opfern von Straftaten sei, „Strafverfolgung und Regress in eigener Regie zu betreiben" (BayLDA, Datenschutzaufsicht hat Juwelier in Fürth Veröffentlichung von Bild- und Videoaufnahmen von Raubüberfall nicht verboten, PE 04.04.2014).

## Twitter kauft Datenauswerter Gnip

Twitter hat Mitte April seinen bisherigen Kooperationspartner, den Datenauswerter Gnip übernommen. Gnip wertet die öffentlichen Daten sozialer Medien wie Twitter, tumblr, Instagram oder Wordpress aus. Analysten glauben, dass Twitter sich neue Geschäftsfelder mit dem Verkauf von Daten erobern will. Twitter erklärte hierzu, die Übernahme von Gnip erlaube es dem Unternehmen, die mehr als 500 Millionen täglichen Tweets besser zu analysieren. Bislang überließ Twitter die Auswertungen anderen Firmen, darunter Gnip.

Es gibt zahlreiche Interessenten für die Datenauswertungen. Finanzfirmen wollen über die Tweets den Puls der Märkte fühlen und Fernsehproduzenten den Vorlieben des Publikums nachspüren. „Öffentliche Tweets erlauben tiefe Einsichten in vielen Bereichen – so sehr, dass Universitäten, Journalisten, Politiker und Unternehmen regelmäßig aufbereitete Twitter-Daten nutzen, um Trends zu erkennen, Stimmungen zu analysieren, mit Kunden in Kontakt zu kommen und Vieles mehr", erklärte Twitter-Vizechefin Jana Messerschmidt.

Twitter hat etwa 250 Millionen registrierte Nutzer. Dieses gewaltige Reservoir hat eine eigene Branche hervorgebracht, die Tweet-Kommunikation nach Trends analysiert. Neben Gnip kooperierte Twitter bislang auch mit Datasift und Dataminr. Diese Firmen erkaufen sich Zugang zu den Tweets, sammeln und bündeln die Daten und verkaufen diese dann an ihre Zielgruppen weiter. (Twitter kauft Datenanalysierer Gnip, www.tagesschau.de, 16.04.2014; Twitter kauft Datenauswerter, www.fr-online.de, 16.04.2014)

# Rechtsprechung

### VerfGH RP

## Steuerdaten-CD-Kauf noch rechtmäßig

Der Verfassungsgerichtshof Rheinland-Pfalz (VerfGH RP) hat mit Urteil vom 24.02.2014 eine Verfassungsbeschwerde gegen die Verwertung einer sog. Steuerdaten-CD, die das Land Rheinland-Pfalz im Jahr 2012 von einer Privatperson erworben hatte, zurückgewiesen (Az. VGH B 26/13). Er setzte aber zugleich der Verwertung einer angekauften Steuerdaten-CD im strafrechtlichen Ermittlungsverfahren Grenzen und mahnte eine stärkere gerichtliche Kontrolle an.

Das angekaufte Datenpaket enthielt zahlreiche Datensätze von Kunden einer Schweizer Bank, unter denen sich auch der Beschwerdeführer befand. Auf der Basis dieser Daten erließ das Amtsgericht Koblenz im Mai 2013 gegen den Beschwerdeführer einen Durchsuchungsbeschluss wegen des Verdachts der Steuerhinterziehung und ordnete nach erfolgter Durchsuchung die Beschlagnahme verschiedener Unterlagen an. Die gegen die Beschlüsse des Amtsgerichts erhobenen Beschwerden wies das Landgericht Koblenz als unbegründet zurück, da nicht von einem Verwertungsverbot auszugehen sei und keine Strafbarkeit der den Datenankauf tätigenden deutschen Beamten vorliege. Hiergegen brachte der Beschwerdeführer vor, die Verwertung der auf der CD vorhandenen Daten verletze ihn in seinem Recht auf ein faires Verfahren, in seinem allgemeinen Persönlichkeitsrecht sowie in seinem Grundrecht auf Unverletzlichkeit der Wohnung.

Der VerfGH RP wies die Verfassungsbeschwerde als unbegründet zurück. Selbst eine rechtswidrige Beweiserhebung führe nicht ohne weiteres zu einem Verwertungsverbot. Für die Beurteilung eines fairen Verfahrens seien in einer Gesamtschau nicht nur die Rechte des Beschuldigten, sondern auch die Erfordernisse einer funktionstüchtigen Strafrechtspflege in den Blick zu nehmen. Zwar gebe es im Strafverfahren keine Wahrheitsermittlung um jeden Preis. So könne die verfassungsrechtliche Grenze überschritten sein, wenn staatliche Stellen bereits die Beweiserhebung allein an den engeren Voraussetzungen eines Beweisverwertungsverbotes ausrichteten. Der Staat dürfe aus Eingriffen ohne Rechtsgrundlage grundsätzlich keinen Nutzen ziehen. Im Hinblick auf den Ankauf von sog. Steuerdaten-CDs gebe es eine unklare Rechtslage. Diese Art der Gewinnung von Beweismitteln weiche deutlich vom Normalfall ab.

Bei greifbaren Anhaltspunkten dafür, dass Informationen in rechtswidriger oder gar strafbarer Weise gewonnen worden seien, sei es erforderlich, dass der Sachverhalt der Informationserhebung hinreichend aufgeklärt werde. Im Falle eines Durchsuchungsbeschlusses seien dem Richter alle entscheidungserheblichen Tatsachen mitzuteilen. Hierzu gehöre auch die Abwägungsentscheidung der Steuerbehörden über den Ankauf der Daten. Gerichte und Strafverfolgungsbehörden müssten gemeinsam die praktische Wirksamkeit des Richtervorbehalts als Grundrechtssicherung gewährleisten. Die Gerichte dürften insbesondere die Frage der möglichen Strafbarkeit deutscher Beamter nicht dahinstehen lassen. Die Prüfungstiefe der angegriffenen Gerichtsentscheidungen und deren tatsächliche Grundlagen seien gerade noch ausreichend gewesen. Namentlich die Annahme, dass sich die deutschen Beamten beim Ankauf der Daten nicht strafbar gemacht hätten, sei im Ergebnis verfassungsrechtlich nicht zu beanstanden. Eine obergerichtliche Klärung dieser Frage stehe gleichwohl noch aus.

Die rechtswidrige oder gar strafbare Erlangung eines Beweismittels durch eine Privatperson führe nur in Ausnahmefällen zur Unverwertbarkeit dieses Beweismittels im Strafverfahren. Es unterliege keinen verfassungsrechtlichen Bedenken, dass die Gerichte in den angegriffenen Entscheidungen das Handeln der Privatperson nicht der staatlichen Sphäre zugerechnet haben. Eine Zurechnung sei verfassungsrechtlich nicht geboten gewesen, da der Anbieter aus eigenem Antrieb gehandelt habe. Die finanzielle Anreizwirkung für den Informanten durch frühere, vereinzelte Ankäufe von Daten-CDs sei jedenfalls zum Zeitpunkt des Ankaufs der CD durch das Land Rheinland-Pfalz noch nicht von derartigem Gewicht gewesen, dass der Informant gleichsam als „verlängerter Arm“ des Staates angesehen werden könne. Der VerfGH RP weist jedoch darauf hin, dass in Zukunft eine Situation entstehen könne, die es als gerechtfertigt erscheinen lasse, das Handeln eines privaten Informanten der staatlichen Sphäre zuzurechnen. Die Gerichte seien daher zukünftig gehalten, zu überprüfen, wie sich das Ausmaß und der Grad der staatlichen Beteiligung hinsichtlich der Erlangung der Daten darstellen. Für die Frage der Zurechnung könne auch ein gegebenenfalls erheblicher Anstieg von Ankäufen ausländischer Bankdaten und eine damit verbundene Anreizwirkung zur Beschaffung dieser Daten von Bedeutung sein.

Der Beschwerdeführer werde nicht in seinem Recht auf informationelle Selbstbestimmung nach Art. 4a der Landesverfassung Rheinland-Pfalz (LV RP) verletzt, da die Verwertung der personenbezogenen Daten die verfassungsrechtliche Pflicht einer wirksamen staatlichen Strafverfolgung und Bekämpfung von Straftaten erfülle sowie der Herstellung von Steuergerechtigkeit und der Gewährleistung eines gesicherten Steueraufkommens diene. Es liege darum auch kein Verstoß gegen das Grundrecht auf Unverletzlichkeit der Wohnung aus Art. 7 Abs. 1 LV RP vor (Verfassungsgerichtshof Rheinland-Pfalz, PM Nr. 6/2014, Verfassungsgerichtshof mahnt stärkere gerichtliche Kontrolle bei der Verwertung einer angekauften Steuerdaten-CD im strafrechtlichen Ermittlungsverfahren an und zeigt Grenzen auf – Verfassungsbeschwerde gleichwohl ohne Erfolg, www.mjv.rlp.de 24.02.2014).

BGH

## Telefonüberwachungsschutz für Anwälte im Anbahnungsverhältnis

Der 3. Strafsenat des Bundesgerichtshofs (BGH) hat mit Beschluss vom 18.02.2014 die Beschwerde des Generalbundesanwalts gegen einen Beschluss des Ermittlungsrichters des BGH als unbegründet verworfen, in dem dieser feststellte, dass die Ermittlungsbehörden es rechtswidrig unterlassen haben, die automatisch gefertigte Aufzeichnung zweier Telefonate unverzüglich zu löschen, die ein Rechtsanwalt zur Anbahnung eines Mandatsverhältnisses geführt hatte (Az. StB 6/13). Entgegen anderslautender Berichte in Presse, Funk und Fernsehen waren diese Aufzeichnungen allerdings nicht bei einer gezielten Abhörmaßnahme gegen den Rechtsanwalt angefallen, sondern stammten aus einer vom BGH-Ermittlungsrichter angeordneten Überwachung des Telefonanschlusses eines Beschuldigten, gegen den der Generalbundesanwalt ein Ermittlungsverfahren wegen des Verdachts der Mitgliedschaft in einer terroristischen Vereinigung im Ausland führt. Auf diesem Anschluss hatte der Rechtsanwalt angerufen, um dem Beschuldigten seine Dienste als Verteidiger anzubieten. Dieses Angebot hatte der Beschuldigte später angenommen.

Der BGH bestätigte, dass der Rechtsanwalt berechtigt ist, das Zeugnis über den Inhalt der beiden Telefonate zu verweigern, obwohl diese nur der Anbahnung des Mandatsverhältnisses mit dem Beschuldigten dienten. Nach der bestehenden Gesetzeslage waren die im Rahmen der Telefonüberwachung des Beschuldigten automatisch gefertigten Aufzeichnungen daher unverzüglich zu löschen. Sie durften insbesondere auch nicht zum Zwecke der späteren gerichtlichen Überprüfung der Rechtmäßigkeit von Anordnung und Vollzug der Überwachungsmaßnahme weiter aufbewahrt werden (Bundesgerichtshof bestätigt Pflicht zur unverzüglichen Löschung aufgezeichneter Telefonate zwischen Verteidigern und Beschuldigten, juris.bundesgerichtshof.de 07.03.2014; Abhörmaßnahmen erschwert, SZ 08./09.03.2014, 5).

BAG

## Beweisverwertungsverbot bei verfrühter Videokontrolle

Das Bundesarbeitsgericht (BAG) hat in einem Urteil vom 21.11.2013 bestätigt, dass die heimliche Videoüberwachung von Arbeitnehmern nur in Ausnahmefällen erlaubt ist (Az. 2 AZR 797/11). Das Videografieren von Arbeitnehmern und der damit verbundene schwere Eingriff in deren allgemeines Persönlichkeitsrecht ist danach nur in Ausnahmefällen und unter bestimmten Voraussetzungen erlaubt. Wer dies nicht beachtet, darf das heimlich gewonnene Material nicht als Beweis für arbeitsrechtliche Verstöße der Mitarbeiter nutzen.

Der Betreiber eines Supermarktes hatte bei der Inventur festgestellt, dass ihm Leergut beziehungsweise rund 7.000 Euro in der Leergutkasse fehlten. Da dem keine Fehlbuchungen zugrunde liegen konnten und auch die Prüfung der Lagerbestände keine Klärung brachte, installierte das Unternehmen im Bereich der Leergutkasse eine Videoüberwachung. Die Filmaufnahmen zeigten, wie eine Mitarbeiterin mehrmals Geld entnahm und einsteckte. Ihr wurde fristlos und vorsichtshalber auch noch ordentlich gekündigt. Die Mitarbeiterin wehrte sich dagegen erfolgreich mit einer Kündigungsschutzklage. Das BAG urteilte, weder die fristlose noch die ordentliche Kündigung dürfe sich auf Beweise aus der heimlichen Videoüberwachung stützen, und hob das Urteil der Vorinstanz, das zumindest die ordentliche Kündigung als rechtmäßig angesehen hatte, auf.

Eine verdeckte Videoüberwachung sei nur erlaubt, wenn ein hinreichender Anlass oder ein konkreter Tatverdacht gegen den Arbeitnehmer besteht. Der allgemeine Verdacht des Diebstahls reiche dafür nicht aus. Der Arbeitgeber sei verpflichtet, zuvor alle anderen Möglichkeiten auszuschöpfen, um den Sachverhalt aufzuklären, z. B. stichprobenartige Überprüfungen im Kassenbereich und Maßnahmen gegen die mögliche Entwendung von Leergut im Lagerraum. Da der Arbeitgeber nicht nachweisen konnte, diese Möglichkeiten ausgeschöpft zu haben, nahm das BAG ein gerichtliches Beweisverwertungsverbot an und wies die Klage an die Vorinstanz zur erneuten Verhandlung zurück. (Sicking, Heimliche Videoüberwachung der Arbeitnehmer, www.heise.de 12.04.2014).

VerfGH Berlin

## Demo-Übersichtsaufnahmen sind zulässig

Der Verfassungsgerichtshof des Landes Berlin (VerfG Berlin) hat mit Urteil vom 11.04.2014 die von 62 Abgeordneten der Oppositionsfraktionen im Abgeordnetenhaus angestrengten Normenkontrollanträge wegen der Änderung des Versammlungsrechts des Landes zurückgewiesen und festgestellt, dass das angegriffene Gesetz ordnungsgemäß zustande gekommen und die Ermächtigung zur Anfertigung von sogenannten Übersichtsaufnahmen durch die Polizei mit der Verfassung von Berlin (VvB) vereinbar sei. Die Antragsteller hatten geltend gemacht, das Gesetz über Aufnahmen und Aufzeichnungen von Bild und Ton bei Versammlungen unter freiem Himmel vom 23.04.2013 (Berliner Versammlungsgesetz) sei nichtig, weil dem Land Berlin die Gesetzgebungskompetenz fehle und die vorgesehene Anfertigung von sogenannten Übersichtsaufnahmen durch die Polizei zu unbestimmt und unverhältnismäßig geregelt sei. Dadurch werde gegen das Grundrecht der Versammlungsfreiheit aus Art. 26 VvB verstoßen.

Der VerfGH Berlin vertritt dagegen die Ansicht, das Berliner Abgeordnetenhaus habe das nach der Föderalismusreform 2006 noch fortgeltende Versammlungsgesetz des Bundes nicht insgesamt ersetzen müssen und einen abgrenzbaren Teilbereich des seither in die Kompetenz der Länder übergegangenen Versammlungsrechts – nämlich Aufnahmen und Aufzeichnungen in Bild und Ton bei Versammlungen unter freiem Himmel – durch Landesgesetz separat regeln können. Die Anfertigung von Übersichtsaufnahmen durch die Polizei (§ 1 Abs. 3 des Gesetzes) verstoße nicht gegen Grundrechte der Verfassung

von Berlin. Diese greifen zwar in die Versammlungsfreiheit ein und können dazu führen, dass sich Einzelne davon abhalten lassen, an Demonstrationen teilzunehmen. Dieser „Einschüchterungseffekt“ beeinträchtigt auch das Gemeinwohl, da die kollektive öffentliche Meinungskundgabe in Versammlungen eine elementare Funktionsbedingung des demokratischen und freiheitlichen Rechtsstaats ist.

Die Regelung sei aber hinreichend bestimmt und verhältnismäßig. Der Eingriff in die Versammlungsfreiheit werde dadurch wesentlich gemildert, dass Übersichtsaufnahmen offen und für jedermann wahrnehmbar erfolgen müssen und nicht aufgezeichnet werden dürfen. Zur Gewährleistung der Offenheit schreibt das Gesetz die unverzügliche Unterrichtung der Versammlungsleitung vor. Zur Wahrnehmbarkeit trage ferner die bisherige Praxis der Berliner Polizei maßgeblich bei, für die Anfertigung von Übersichtsaufnahmen eigenes Personal und eine eigene Technik einzusetzen. Außerdem würden die eingesetzten Beamten regelmäßig geschult. Die kontinuierliche Überprüfung und Weiterentwicklung aller organisatorischen Maßnahmen und technischen Möglichkeiten zur grundrechtsschonenden Anwendung der gesetzlichen Ermächtigung sei in erster Linie Aufgabe der vollziehenden Gewalt, die dabei der Kontrolle durch die Fachgerichte unterliegt. Im Übrigen trifft den Gesetzgeber in Bezug hierauf und in Bezug auf das ganze Gesetz eine Beobachtungs- und Überprüfungsobliegenheit sowie ggf. eine Nachbesserungspflicht.

Übersichtsaufnahmen seien nur zulässig, wenn sie wegen der Größe oder der Unübersichtlichkeit der Versammlung im konkreten Einzelfall zur Lenkung und Leitung des Polizeieinsatzes erforderlich sind. Der VerfGH Berlin weist darauf hin, dass Übersichtsaufnahmen keine stets zulässige Maßnahme darstellen, sondern zumindest eine abstrakte Gefahrenprognose erfordern. Daraus müssen sich Anhaltspunkte für ihre Notwendigkeit ergeben. Andere gleich geeignete mildere Mittel als die Anfertigung offener Übersichtsaufnahmen ohne Aufzeichnung seien nicht erkennbar, auch die vom Gesetzgeber verworfene mündliche Übermittlung von Lagebildern durch Beamte vor Ort.

Die Entscheidung ist mit 8:1 Stimmen ergangen. Ein Richter des Verfassungsgerichtshofes hat dem Urteil eine abweichende Meinung angefügt (Ermächtigung zu Übersichtsaufnahmen bei Versammlungen unter freiem Himmel verfassungsgemäß, www.berlin.de/sen/justiz/gerichte/lverfgh/ 11.04.2014).

### OVG Berlin-Brandenburg

## Snowdens Asylgesuch wegen Datenschutz nicht öffentlich

Auf die Beschwerde eines Journalisten gegen einen negativen Eilbeschluss des Verwaltungsgerichts (VG) Berlin hin entschied das Oberverwaltungsgericht (OVG) Berlin-Brandenburg mit Beschluss vom 10.12.2013, dass die Bundesregierung nicht die Frage beantworten muss, ob ein Asylgesuch von Edward Snowden an Deutschland mit demjenigen an Polen gerichteten Gesuch identisch ist (Az. 6 S 36.13). Dies gebiete der Schutz der Privatsphäre von Edward Snowden, der dem öffentlichen Interesse an dieser Information vorgehe. Edward Snowden hatte selbst der Öffentlichkeit bekannt gegeben, dass er in mehreren Ländern Asyl beantragt hat. Der Text seines Antrags an die polnische Regierung ist in der Öffentlichkeit bekannt. Mitglieder der deutschen Bundesregierung hatten kurz nach Eingang seines Gesuchs in Berlin erklärt, Snowden könne nicht nach Deutschland kommen (ANA-ZAR 1/2014, 11).

### OVG Schleswig

## Datenschutzbehörden dürfen ihre Meinung äußern

Mit Beschluss vom 04.03.2014 gab das Oberverwaltungsgericht (OVG) Schleswig dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) auf dessen Beschwerde gegen einen Beschluss des Verwaltungsgerichts (VG) Schleswig in wesentlichen Punkten Recht (Az. 8 B 50/13). Zuvor hatte das VG mit Beschluss vom 05.11.2013 dem ULD verboten, die Datenverarbeitung eines bundesweit agierenden bayerischen Apothekenrechenzentrums zu kritisieren (Az. 4 MB 82/13).

Hintergrund der OVG-Entscheidung ist eine langjährige bundesweite Praxis von Apothekenrechenzentren, Rezeptdaten nicht nur zur Abrechnung gegenüber Krankenkassen zu nutzen, sondern diese – gekennzeichnet über sog. „Arzt-„ und „Patientenanonyme“ – an medizinische Informationsdienstleister zu verkaufen, die diese Daten dann aufbereitet u. a. an die Pharmaindustrie weitergeben. Norddeutsche Datenschutzaufsichtsbehörden, u. a. das ULD, kritisierten diese Praxis, weil nach ihrer Überzeugung keine hinreichende, gesetzlich geforderte Anonymisierung erfolgt sei. Dies veranlasste das Norddeutsche Apothekenrechenzentrum (NARZ) in Bremen, sein Verfahren zu ändern und nur noch durch Aggregation anonymisierte Rezeptdaten herauszugeben. Demgegenüber veränderte der bayerische Anbieter VSA mit Billigung der dort zuständigen Aufsichtsbehörde, des Bayerischen Landesamtes für Datenschutzaufsicht in Ansbach, seine Datenweitergabe insofern nicht, dass weiterhin mit einem „Patientenanonym“ gekennzeichnete Rezeptdatensätze einzelner Patientinnen und Patienten abgegeben wurden. Der Leiter des ULD kritisierte dies auf Anfrage verschiedener Pressemedien Ende August 2013. Durch den Beschluss des VG Schleswig wurde dem ULD diese Kritik auf Antrag der VSA untersagt mit dem Argument, für die aufsichtliche öffentliche Bewertung sei die lokale Behörde zuständig. Andere Aufsichtsbehörden dürften ihre abweichende Meinung lediglich im behördeninternen Diskurs zur Geltung bringen.

Die Entscheidung des VG wurde nun vom OVG in zweiter und letzter Instanz in wesentlichen Punkten aufgehoben. Das ULD habe generell eine Befugnis zu Presseäußerungen bei einem begründeten Gefahrenverdacht für den Schutz persönlicher Daten. Das ULD habe aber die hierbei gebotene Sachlichkeit und Verhältnismäßigkeit zu wahren. Es müsse in seinen Äußerungen durch entsprechend zurückhal-

tende Formulierungen berücksichtigen, dass die zuständige Aufsichtsbehörde (hier in Bayern) eine Prüfung mit positivem Ergebnis durchgeführt habe. Daher müsse die schleswig-holsteinische Datenschutzbehörde ihre Kritik (z. B.: „die Antragstellerin gebe keine anonymisierten, sondern pseudonymisierte Daten heraus“) als eigene Auffassung kennzeichnen. Mit unangemessen verabsolutierenden, skandalisierenden oder diskreditierenden Bewertungen (z. B.: „das Geschäftsmodell der Antragstellerin sei illegal“) werde der Bereich zulässiger medienöffentlicher Äußerungen über das von der bayerischen Aufsichtsbehörde akzeptierte Verfahren der Datenaufbereitung verlassen.

Die VSA sieht sich als Sieger in der gerichtlichen Auseinandersetzung: „Keine der Aussagen hätte (Weichert) in der damals gewählten Form aufstellen dürfen.“ Sie behauptet weiter, den „vermeintlichen Datenskandal“ habe es gar nicht gegeben. Dagegen meinte Thilo Weichert: „Das Oberverwaltungsgericht hat den Maulkorb, der dem ULD vom Verwaltungsgericht verpasst wurde, wieder abgenommen. Dadurch ist eine qualifizierte – auch kontroverse – öffentliche Datenschutzdebatte in Deutschland weiterhin möglich. Ohne diese Debatte könnten sich Stellen mit dem Verweis auf nicht transparente Prüfergebnisse der lokalen Aufsicht einer öffentlichen Kritik entziehen. Für das ULD ist die OVG-Entscheidung aber nur ein halber Sieg: Das Gericht beschäftigte sich nicht mit der zentralen datenschutzrechtlichen Frage, wann eine hinreichende Anonymisierung in Apothekenrechenzentren vorliegt. Diese Grundsatzfrage muss dringend geklärt werden, um eine Marktverzerrung bei Apothekenrechenzentren zu verhindern und einen effektiven Schutz der hochsensiblen Rezeptdaten zu gewährleisten. Geringerer Datenschutz sollte nicht zum Wettbewerbsvorteil werden“ (OVG Schleswig: Medienäußerungen des Landesdatenschutzbeauftragten zu bayerischem Apothekenrechenzentrum nur eingeschränkt zulässig, PE 04.03.2014; ULD, OVG Schleswig: Kein Maulkorb für das ULD, PE 05.03.2014; VSA, OVG weist Weichert in die Schranken, PE 05.03.2014).

### HessLAG

## Datenlöschung rechtfertigt fristlose Kündigung

Das Hessische Landesarbeitsgericht (HessLAG) hat mit Urteil vom 05.08.2013 entschieden, dass die fristlose Kündigung eines Account-Managers aufgrund eigenmächtiger Löschung zahlreicher Daten von seinem Benutzer-Account im Betrieb gerechtfertigt ist (Az. 7 Sa 1060/10). Die Datenlöschung stelle einen so erheblichen Verstoß gegen selbstverständliche Nebenpflichten aus dem Arbeitsvertrag dar, dass die sofortige Beendigung des Arbeitsverhältnisses nicht zu beanstanden sei.

Der Kläger war seit Anfang 2009 bei einem Unternehmen der EDV-Branche in Frankfurt als Account-Manager beschäftigt. Nach den Ermittlungen eines gerichtlich eingesetzten Sachverständigen hatte er am 29. und 30.06.2009 von seinem Benutzer-Account im Betrieb ca. 80 eigene Dateien gelöscht und weitere 374 Objekte, nämlich 144 Kontakte, 51 E-Mails, 167 Aufgaben und 12 Termine. Hintergrund waren laufende Verhandlungen der Parteien um die Abänderung bzw. Aufhebung seines Arbeitsvertrages. Am 01.07.2009 entdeckte die Arbeitgeberin die Löschungen und kündigte dem Kläger fristlos, hilfsweise ordentlich zum 31.08.2009.

Das Arbeitsgericht Frankfurt/Main hielt in erster Instanz die Kündigung nur als ordentliche Kündigung für gerechtfertigt. Das HessLAG war dagegen der Ansicht, das Fehlverhalten des Klägers rechtfertige die fristlose Kündigung.

Eigenmächtige Datenlöschungen rechtfertigten eine sofortige Beendigung des Arbeitsverhältnisses. Die erfolgte umfangreiche Datenlöschung habe das Vertrauen in die Integrität des Klägers vollständig zerstört. Die Daten stünden in der Verfügungsmacht des Arbeitgebers. Eine eigenmächtige Löschung durch einen Arbeitnehmer mit den sich daraus ergebenden internen Problemen und gegenüber Kunden sei ein so erheblicher Verstoß gegen selbstverständliche Nebenpflichten aus dem Arbeitsvertrag, dass die sofortige Beendigung des Arbeitsverhältnisses gerechtfertigt sei. Eine Abmahnung, die in der Regel einer Kündigung aus verhaltensbedingten Gründen vorangehen muss, sei hier nicht notwendig gewesen. Der Kläger habe genau gewusst, dass die Löschung der Daten von der Arbeitgeberin auf keinen Fall hingenommen werden würde (Löschung von Daten rechtfertigt fristlose Kündigung eines Account-Managers, www.kostenlose-urteile.de 07.03.2014, Daten gehören Arbeitgeber, SZ 05.08.2014, 25).

### LAG RP

## Schmerzensgeld bei Videokontrolle

Das Landesarbeitsgericht Rheinland-Pfalz (LAG RP) hat mit Urteil vom 23.05.2013 entschieden, dass ein Mitarbeiter Anspruch auf Schmerzensgeld hat, wenn er rechtswidrig per Video überwacht wurde (Az. 2 Sa 540/12). Videoüberwachung sei eine Verletzung des allgemeinen Persönlichkeitsrechts. Der Arbeitgeber hatte die Kontrolle damit begründet, dass es zuvor zum Diebstahl von Firmeneigentum gekommen sei. Diese Behauptung war für das LAG RP zu pauschal. Der Mitarbeiter erhält 650 Euro Schmerzensgeld - statt der geforderten 10.000 Euro. Der Kläger hatte diese hohe Summe verlangt, weil er wegen der Überwachung an Durchfall, Erbrechen und Unwohlsein gelitten habe und zum Arzt musste. Das LAG RP sah dagegen keinen nachvollziehbaren Zusammenhang zwischen Überwachung und behaupteten Krankheitssymptomen (Anspruch auf Schmerzensgeld Videoüberwachung, www3.mjv.rlp.de 23.05.2013).

### LG Frankfurt/Main:

## Nutzende müssen Webanalyse-Tool widersprechen können

Gemäß einem Urteil des Landgerichts (LG) Frankfurt vom 18.02.2014 auf die Klage eines Wettbewerbers hin muss ein Betreiber einer Internetseite die Nutzenden deutlich sichtbar über Widerspruchsmöglichkeiten beim Einsatz des Webanalyse-Tools Piwik informieren

(Az. 3-10 O 86/12). Der Hinweis muss auch dann erfolgen, wenn der Webseitenbetreiber das Piwik-Plugin AnonymizeIP einsetzt. Da Piwik mit Hilfe anderer Daten dennoch pseudonymisierte Profile erstelle, müssen die Nutzenden darauf hingewiesen werden und dem Einsatz widersprechen können. Das Gericht verweist zur Begründung auf den Beschluss des Düsseldorfer Kreises vom 27.11.2009 über die „datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internetangeboten.“ Diese Vorgaben würden durch die Anonymisierung der IP-Adresse noch erfüllt. Allerdings müssen nach § 15 Abs. 3 Telemediengesetz (TMG) die Seitenbesucher die Möglichkeit haben, der Bildung pseudonymisierter Nutzungsprofile zu widersprechen. Zudem müssen die Nutzer über ihr Widerspruchsrecht informiert werden.

Nach Ansicht des Gerichts gilt dies auch im konkreten Fall, weil der beklagte Webseitenbetreiber „bei der Erstellung der Nutzungsprofile mit Hilfe des Programms Piwik - entgegen der vom Hersteller selbst gewählten Begrifflichkeit - Pseudonyme im Sinne des § 15, Abs. 3 TMG verwendet“. Die Richter berufen sich dabei auf eine Einschätzung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holsteins (ULD). Das ULD hatte Piwik getestet und im März 2011 eine ausführliche Stellungnahme zur Nutzung des Programms verfasst. Demnach benutzt Piwik „eine Heuristik, die versucht, einen Besucher mit einem vorherigen Besuch zu identifizieren, indem bestimmte Daten berücksichtigt werden. Insbesondere sind dies die IP-Adresse, die Auflösung, der Browser, die verwendeten Plugins und das Betriebssystem“. Die Daten würden kombiniert und zu einem Hashwert verrechnet, wobei selbst bei einer Nutzung von AnonymizeIP die vollständige IP-Adresse in den Hashwert einfließe. Das ULD kam zu dem Schluss: „Die Wiedererkennbarkeit von Internetnutzern hängt zudem nicht unbedingt an der IP-Adresse, sondern kann mit überraschend großer Zuverlässigkeit auch über andere Werte vorgenommen werden.“

In seinem Urteil übernimmt das Gericht diese Auffassung. Aufgrund dieser Piwik-Funktion müsse der Webseitenbetreiber deutlich auf die Widerspruchsmöglichkeit der Analyse hinweisen. Möglich sei ein Pop-up oder ein „deutlich hervorgehobener Hinweis mit einem Hyperlink auf der Startseite“. Es sei nicht ausreichend, wie im konkreten Fall die Datenschutzbestimmungen auf der Kontaktseite zu platzieren. Gemäß dem ULD wird der Widerspruch bei Piwik „in Form eines Opt-out-Cookies abgelegt, so dass beispielsweise nach einem Löschen aller Cookies das Opt-out erneut erklärt werden muss.“ Der Leiter des ULD Thilo Weichert begrüßte das Urteil und wies darauf hin, dass es sich bei Piwik noch um das möglicherweise „datenschutzfreundlichste“ Analyseverfahren handele. Andere Tools wie Google Analytics seien in Sachen Datenschutz erheblich problematischer. Es komme darauf an, Piwik so zu installieren, dass die Vorgaben des Telemediengesetzes eingehalten werden.

Piwik ist ein Open-Source-Programm für Webanalytik und wurde nach Angaben der Betreiber fast 1,7 Millionen Mal heruntergeladen. Anders als bei Google Analytics verbleiben die Daten auf den Servern des Betreibers. Zu den Nutzern gehören unter anderem T-Mobile, Wikimedia Deutschland, Forbes und Sharp. Auch die neue französische Suchmaschine Qwant verwendet Piwik, ohne ihre Nutzer darauf hinzuweisen (Nutzer müssen Piwik-Analyse widersprechen können, www.golem.de 11.03.2014).

### OLG Koblenz

## Ex-Partner muss Intim-Fotos löschen

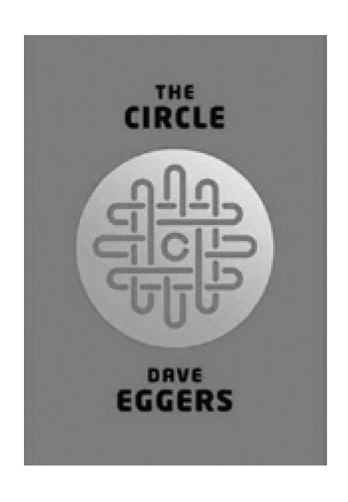
Das Oberlandesgericht (OLG) Koblenz entschied mit Urteil vom 20.05.2014, dass nach Ende einer Beziehung Intimfotos des früheren Partners von Datenträgern gelöscht werden müssen. Die während einer Beziehung im Einvernehmen erfolgte Fertigung von Lichtbildern und Filmaufnahmen stelle zwar keinen rechtswidrigen Eingriff in das Persönlichkeitsrecht der abgebildeten Person dar. Die insofern anzunehmende Einwilligung habe auch zum Inhalt, dass der Andere die Aufnahmen im Besitz hat und über sie verfügt. Der Widerruf des Einverständnisses sei aber nicht ausgeschlossen, wenn aufgrund veränderter Umstände dem allgemeinen Persönlichkeitsrecht der Betroffenen Vorrang vor dem Umstand zu gewähren ist, dass sie der Anfertigung der Aufnahmen zu irgend einem Zeitpunkt zugestimmt hat. Das ist nach Ansicht des OLG nach Beendigung der Beziehung der Fall, wenn es sich um intime und damit den Kernbereich des Persönlichkeitsrechts betreffende Aufnahmen handelt. Der Anspruch auf Löschung digitaler Fotografien und Videoaufnahmen ist auf diesen Bereich beschränkt. Das OLG Koblenz bestätigte damit das erstinstanzliche Urteil. Im vorliegenden Fall streiten die Parteien aus dem Lahn-Dill-Kreis über die Verwendung von Lichtbildern und Filmaufnahmen. Der Beklagte ist Fotograf. Während der zwischenzeitlich beendeten Beziehung wurden einvernehmlich zahlreiche Bildaufnahmen der Klägerin gefertigt, darunter auch intime Aufnahmen, die sie - teilweise selbst gefertigt - dem Beklagten in digitalisierter Form überlassen hat.

Die mit der Klage geltend gemachten Ansprüche es zu unterlassen, die Aufnahmen Dritten oder der Öffentlichkeit zugänglich zu machen, hatte der Beklagte anerkannt. Das Landgericht (LG) hat den Beklagten darüber hinaus verurteilt, die in seinem Besitz befindlichen elektronischen Vervielfältigungsstücke von intimen Aufnahmen der Klägerin vollständig zu löschen. Soweit die Klägerin darüber hinausgehend die vollständige Löschung sie zeigender Aufnahmen beansprucht hat, hatte das LG die Klage abgewiesen. Der Beklagte hatte gegen die teilweise Verurteilung zur Löschung Berufung eingelegt, die Klägerin ihrerseits gegen die Ablehnung einer vollständigen Löschung. Der zuständige 3. Zivilsenat des OLG bestätigte die Entscheidung des LG in vollem Umfang.

Zwar habe die Klägerin in die Erstellung und Nutzung der Lichtbilder eingewilligt. Soweit es sich um intime Aufnahmen handele, sei die Einwilligung jedoch zeitlich auf die Dauer der zwischen den Parteien bestehenden Beziehung beschränkt worden. Die Einwilligung könne widerrufen werden, da das den Kernbereich des Persönlichkeitsrechts betreffende Interesse der Klägerin an der Löschung der Aufnahmen höher zu bewerten sei als das Eigentumsrecht des Beklagten an der Existenz der Auf-

nahmen. Da es sich um Bild- und Filmaufnahmen für den privaten Bereich gehandelt habe, werde auch das berufliche Tätigkeitsfeld des Beklagten nicht beeinträchtigt. Die vollständige Löschung könne hingegen bei einer Abwägung der Persönlichkeitsrechte der Klägerin mit den Eigentumsrechten auf Seiten des Beklagten nicht beansprucht werden. Anders als bei intimen Aufnahmen seien Lichtbilder, welche die Klägerin im bekleideten Zustand in Alltags- oder Urlaubssituationen zeigten, in einem geringeren Maße geeignet, ihr Ansehen gegenüber Dritten zu beeinträchtigen. Es sei allgemein üblich, dass Personen, denen die Fertigung von Aufnahmen bei Feiern, Festen und im Urlaub gestattet werde, diese auf Dauer besitzen und nutzen dürfen (Nach Liebesaus - kein umfassender Anspruch auf Löschung von überlassenen Dateien mit eigenen Foto- und Videoaufnahmen, www.kostenlose-urteile.de 20.05.2014).

# Buchbesprechungen




Dave Eggers
**The Circle - an novel**
Alfred A. Knopf Mcsweeney´s Books, San Francisco, 2013, 491 S., ISBN 978-0-385-35139-3

(TW) Im April 2014 erklärte Springer-Chef Mathias Döpfner in einem offenen Brief, dass sein Unternehmen sich in totaler Abhängigkeit des Internet-Konzerns Google befände. Die Kooperation der deutschen Zeitungsverlage könne man „schizophren“ oder auch “alternativlos” nennen. Google habe inzwischen das „globale Netzmonopol“ und wolle einen „Supra-Staat“ errichten; seine Macht betreffe die Zukunft Europas (SZ 17./18.04.2014, 14). Was Döpfner anspricht, hat Eggers – auf der Basis unserer Erfahrungen mit Google, Apple, Facebook und Amazon, den Silicon-Valley-Oligopolisten – in seiner Distopie weitergedacht. Die Oligopolisten sind inzwischen von einem Unternehmen „The Circle“, dem weltweiten Informationstechnik-Monopolisten, geschluckt worden, der nicht nur Konsumenten und Wirtschaft, sondern auch die Politik weltweit in die Tasche steckt.

Es geht nicht mehr um den allüberwachenden staatlichen Big Brother im Sinne von George Orwells „1984“; sondern um ein von drei „weisen Männern“ geführtes Unternehmen, dessen Geschäftsmodell es ist, alles transparent zu machen. „TruYou“ schafft eine Identität für alle Netzaktivitäten und bereinigte das Netz auch von allem, was dort im Schutz der Anonymität vor sich ging. Kriminalität ist dabei, beseitigt zu werden. Individuelle und kollektive Selbstoptimierung per Quantified Self und durch weltweit von Nutzenden installierter Videobeobachtung - auch per Drohne – verschafft den wissenschaftlich begründeten Durchblick. Und alles potenziert die Macht des Netzgiganten. Damit liefert „The Circle“ die Blaupause der idealen „Demokratie“, von der die Post-Privacy-Ideologen, die Vertreter der sog. Spackeria, schwadronieren, in der alle Menschen alles wissen (können sollen). Eggers denkt – ohne Katastrofen-Szenario – diese Distopie auf der Basis der heute schon verfügbaren Technologien konsequent weiter. Nicht thematisiert wird von ihm die technologisch noch nicht ganz gelöste Thematik der Energieversorgung und der weiterhin nicht unbeschränkten Datenspeicherkapazität.

Anders als bei Orwell gibt es bei Eggers keinen rebellierenden Helden (mehr). Hauptperson ist Mae, die über Beziehungen zum Circle kommt und von untergeordneten Serviceaufgaben in die Führungsetage des Circle aufsteigt als Unternehmens-Botschafterin, die mit einer dauernd auf Sendung befindlichen Webcam dem Publikum Produkte, Ideologie und Zuneigung vermittelt. Mae ist sympathisch, kommt aus kleinen Verhältnissen, ist abenteuerlustig (paddelt gerne) und entwickelt fast naturwüchsig die Philosofie des Circles, die in drei knappen Botschaften zusammengefasst werden kann: „Geheimnisse sind Lügen“, „Teilen heißt Fürsorgen“, „Privatheit ist Diebstahl“ (Secrets are Lies, Sharing is Caring, Privacy is Theft).

Angesporn von diesen Ideen und ihrem Ehrgeiz nimmt sie in Kauf, dass ihr nahe stehende Menschen, die den Weg in die transparente Zukunft (teilweise) nicht mitgehen können oder wollen, untergehen. Was unspektakulär mit der Einstellung Maes im Circle beginnt, nimmt Fahrt auf und eskaliert. Auch wenn das Ziel der Allwissenheit am Ende nicht erreicht wird – die Träume der im Koma liegenden Freundin von Mae bleiben unentdeckt – so bleibt doch Beklemmung. Auch insofern stellt sich Eggers in die Tradition Orwells. Diese Beklemmung nährt sich aus all dem, was wir heute im und mit dem Internet erleben. Die Fiction des Circle bleibt auf Augenhöhe zu den heutigen technischen, ökonomischen und politischen Realitäten. Die willfährige Rolle vieler Politiker öffnet Einsicht in aktuelle (nicht nur US-amerikanische) Mechanismen. Dialektischer Optimismus wird nicht bedient, wohl aber der Wunsch nach spannender Unterhaltung. Leider ist das Buch noch nicht ins Deutsche übersetzt. Wer hierauf nicht warten will, wird auch das englischsprachige Original „liken“ – ohne zu klicken.




Harding, Luke
**Edward Snowden**
Geschichte einer Weltaffäre
Edition Weltkiosk, London Berlin 2014, 277 S. ISBN 978-3-942377-09-6

(TW) Es ist ein Glück für alle Menschen, denen der Datenschutz am Herzen liegt, dass der Whistleblower Edward Snowden, der Licht in die Überwachungsaktivitäten der Geheimdienste der USA und Großbritanniens – National Security Agency (NSA) und Government Communikations Headquarters (GCHQ) – brachte, ein fachlich ungemein kompetenter, uneitler, gewissenhafter, strategisch denkender und ebenso handelnder Mensch ist, der sich von einem US-amerikanischen Patriot zu einem global denkenden Bürgerrechtler entwickelt hat. So konnte er professionell tausende hochgeheimer aussagekräftiger NSA-Dokumente sichern, eine filmreife Flucht durchführen und durch die Einschaltung von kritischen und unabhängigen Journalisten gewährleisten, dass einerseits die kriminellen und grundrechtszerstörenden Machenschaften zweier westlicher Geheimdienste aufgedeckt werden und dass zugleich Schaden für die öffentliche Sicherheit oder für Personen vermieden wird.

Diese bedachte Vorgehensweise hat einen weiteren Effekt. Es wurden nicht nur qualifizierte Presseberichte initiiert, die eine globale politische Debatte auslösten. Die eingeschalteten Journalisten führten vielmehr auch systematische Recherchen durch, die Wissenschaftlern größte Ehre bringen würden, und veröffentlichten dann thrillermäßig geschriebene umfassende Darstellungen in Buchform, die die Ereignisse von der Flüchtigkeit der Tagespresse befreien und in das dauernde Gedächtnis der Bibliotheken retten.

Die erste solche Darstellung in Buchform stammt von dem britischen Guardian-Reporter Luke Harding, der u. a. auch ein Buch über „Wikileaks – Julian Assanges Krieg gegen Geheimhaltung“ verfasste. Harding beschreibt die Geschichte Edward Snowdens von seiner Kindheit und Jugend an der Ostküste der USA über sein Engagement bei der Armee und seine erste Geheimdiensttätigkeiten, u. a. für die CIA und in der Schweiz, bis hin zu seiner Beschäftigung als Zivilangestellter zunächst bei Dell, dann bei Booz Allen Hamilton für die NSA, u. a. in Japan, letztlich auf Hawai, wo er – in Erkenntnis des Unrechts der durchgeführten globalen Überwachung – systematisch Dokumente sammelte, die er nach einer spektakulären Flucht nach Hongkong Journalisten zukommen ließ, die diese auswerteten und öffentlich zugänglich machten. Der Autor zeichnet ein sehr persönliches Bild von Snowden, analysiert seine Entwicklung im Rahmen seiner Arbeits- und Lebensumstände von Maryland bis nach Russland, wo er vorläufig Asyl gefunden hat, vom eher konservativ eingestellten Nerd bis zum kühl berechnenden und zugleich glühenden Bürgerrechtler. Er wählt dabei die Form des Romans, der von Anfang an bis über das Buchende hinaus spannend ist. Er schreibt aus der Perspektive des britischen Journalisten für den Guardian, der Zeitung, die die Enthüllungen immer wieder vorangetrieben hat, und beleuchtet insbesondere auch die Aktionen des GCHQ und der britischen Regierung. Er schildert anschaulich die Erkenntnisse über die technischen Überwachungsmethoden in Bezug auf den globalen Internetverkehr und die vielen betroffenen Staaten, Organisationen, Unternehmen und Menschen, von den Vereinten Nationen, über Indonesien und Brasilien bis nach Deutschland. Alan Rusbridger, Chefredakteur des Guardian, verfasste ein Vorwort. Von den drei Snowden-Büchern ist das von Harding das romanhafteste und deshalb am leichtesten zu lesende, ohne dass dadurch technische und politische Fakten und Analyse zu kurz kämen (vgl. auch Harding, Liebe NSA: Wie finden Sie mein Buch? SZ 21.04.2014, 11).




Rosenbach, Marcel/Stark, Holger
**Der NSA Komplex**
Edward Snowden und der Weg in die totale Überwachung
Deutsche Verlags-Anstalt München, Spiegel Buchverlag Hamburg, 2014, 383 S. ISBN 978-3-421-04658-1

(TW) Während das Buch von Luke Harding an das internationale Publikum gerichtet ist und Edward Snowden und dessen Enthüllungsaktion in den Vordergrund stellt, werfen die Autoren und Spiegeljournalisten Marcel Rosenbach und Holger Stark einen eher spezifisch deutschen Blick auf die durch Snowden ermöglichten Enthüllungen. Diese Darstellung ist eingerahmt von der Geschichte der Tätigkeiten, die Snowdens für die National Security Agency (NSA) erbracht hat, und seiner Flucht nach Hongkong und dann weiter nach Moskau. Sie schließt mit einer Bewertung von Snowdens Verdiensten und seiner persönlichen Perspektiven. Im Mittelpunkt aber steht die systematische Darstellung der NSA-Überwachungsaktivitäten und welche Bedeutung diese für die deutsche Politik haben. Dabei wird das „Merkel-Gate“ ausführlich dargestellt und wie die Interaktion zwischen den USA und Deutschland stattfand und weiterhin erfolgt. Die Autoren stellen die für viele Einzelberichte vorgenommenen Dokumenten-Recherchen in einen umfassenderen Zusammenhang und liefern damit schon fast eine systematische Analyse der NSA. Nicht nur das: Sie nehmen eine Analyse der globalen Risiken vor, die sich aus der digitalen Überwachbarkeit ergeben. Damit macht sich das Buch zur Pflichtlektüre nicht

nur für jeden Bundestagsabgeordneten im NSA-Untersuchungsausschuss, sondern auch für jedes Parlaments- und Regierungsmitglied.

Das Buch kombiniert die Vorzüge einer flüssig und leicht geschriebenen und zugleich spannenden Tatsachenstory mit der akribischen Auswertung von Originaldokumenten und der Wiedergabe von Rechercheergebnissen. Es ist auch geeignet als Nachschlagewerk, das in einem über 60seitigen Anhang eine Chronologie der Snowden-Enthüllungen bis Februar 2014 enthält, ein Glossar von Abkürzungen und Fachbegriffen, einen umfangreichen Endnotenapparat mit Quellennachweisen und ein leicht erschließbares Stichwortregister (dies fehlt leider bei den Büchern von Harding und Greenwald zum gleichen Thema). Durch die Darstellung der größeren Zusammenhänge der Internet-Überwachung schärft das Buch nicht nur für Spezialisten das Bewusstsein über den technischen und politischen Kontext, sondern auch für eine eher belletristisch interessierte Leserschaft. Also: Zur Lektüre für alle dringend zu empfehlen (vgl. auch Schultz, Die Gedanken sind frei, SZ 15.04.2014, 13).




Glenn Greenwald
**Die globale Überwachung**
Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen
Droemer Verlag München 2014, 366 S.
ISBN 978-3-426-27635-8

(TW) Glenn Greenwald, der in Rio/Brasilien wohnende US-amerikanische Publizist und Verfassungsrechtler, ist neben Snowden selbst wohl die wichtigste Person in der Enthüllungsgeschichte: Er wurde schon früh von Snowden als sein Sprachrohr ausgesucht, nahm gemeinsam mit der Dokumentarfilmerin Laura Poitras den Kontakt zu dem nach Hongkong geflohenen Whistleblower auf, analysierte die Originaldokumente und veröffentlichte zunächst insbesondere im Guardian die Enthüllungen. Er war und ist – da Snowden in seiner Bewegungsfreiheit massiv eingeschränkt ist – nicht nur der Vermittler der Fakten, sondern auch für die daraus zu ziehenden Schlussfolgerungen. Seine Zusammenfassung in einem Buch – übersetzt aus dem Englisch „No Place to Hide“ – ist in vieler Hinsicht ein Juwel: Er beschreibt die Kontakte zu Snowden bis zum Abflug aus Hongkong aus erster Hand und in einem kaum an Spannung zu überbietenden Erzählstil. Dann dokumentiert er ausführlich an Hand vieler abgedruckter Dokumente, die ins Deutsche übersetzt sind, detailliert und systematisch die Bespitzelungsaktivitäten von NSA, GCHG und den befreundeten anderen Diensten von den Five Eyes. Dabei werden Passagen, die nationale Sicherheitsinteressen beeinträchtigen könnten, unkenntlich gemacht. Greenwald liefert dem folgend eine tiefgreifende und detaillierte Analyse, was die Massenüberwachung mit uns Menschen und mit unserem demokratischen System macht. Letztlich beschreibt er, welche zentrale Funktion Journalisten für die Kontrolle der Geheimdienste und insbesondere der US-Regierung haben und wie die US-Medien in diesem konkreten Zusammenhang systematisch versagen. Er beschreibt eindringlich, welche affirmative Rolle die etablierten Medienhäuser in den USA mit ihrer angeblich so objektiven Berichterstattung spielen.

Greenwalds Buch ist zum einen eine höchstrelevante Dokumentation für PolitikerInnen, GeheimdienstlerInnen, BürgerrechtlerInnen und kritische Menschen überall auf der Welt, zugleich aber auch ein äußerst einfühlsamer Betroffenenbericht und letztlich ein Manifest für die Verteidigung der Menschenrechte in unserer globalen Informationsgesellschaft. Der Autor schafft es, bei allem Engagement einen objektiven Blick auf die Dienste und die US-Politik zu werfen, wobei diese schonungslos hinsichtlich ihrer Interessen, ihrer Propaganda und ihrer realen Vorgehensweisen, auch gegen Aufklärer wie er selbst, demaskiert werden. Das Buch liefert genug an Beweisen, um die letzten Zweifel an der Faktizität der Internetüberwachung und der damit verbundenen Grundrechtsbeeinträchtigungen durch NSA und GCHQ zu zerstreuen. JedeR, der – voreilig oder interessenbegründet – Snowden einen Verräter oder Verbrecher bezeichnet, sollte im Interesse der Redlichkeit veranlasst, ja gezwungen werden, dieses Buch zu lesen. Das Buch ist insbesondere für BürgerrechtlerInnen eine Ermutigung zum Weiterkämpfen: Wir brauchen viele Snowdens und Greenwalds, um die globale Informationsgesellschaft zu einer humanen zu machen. Den Interessen, die dem entgegen stehen, kann etwas erfolgreich entgegengesetzt werden: Das sind Fakten und Argumente.




Vorratsdaten kann man nach Bedarf fälschen.
Geheimdienste wissen, wie es geht.
0046-742-6899
145-8833512
Grafik: Frans Valenta, Bonn